IN THE SUPREME COURT OF INDIA
[CRIMINAL APPELLATE JURISDICTION]

SPECIAL LEAVE PETITION (CRL.) NO. OF 2014

[Against the Impugned interim order dated 26.02.2014 of the High Court of Bombay at Goa in Criminal Writ Petition No. 10 of 2014.]

IN THE MATTER OF:

UNIQUE IDENTIFICATION AUTHORITY OF INDIA & ANR.. ...PETITIONERS

VERSUS

CENTRAL BUREAU OF INVESTIGATION & ANR. ..RESPONDENT

VOLUME-II

WITH

CRL.MP.NO._____OF 2014

[An application for exemption from filing Certified Copy of Impugned Order and Judgement]

PAPER BOOK

[FOR KINDLY SEE INSIDE]

ADVOCATE FOR THE PETITIONERS: .D.S. MAHRA.

INDEX

SL. NO.	PARTICULARS	PAGE NOS.
14.	ANNEXURE:P-9 A true copy of Criminal Misc. Appln.No.172/2013/C in Case No. RC 7(S)/2013/CBI/ACB/Goa dated 21.10.2013	270-272
15.	ANNEXURE:P-10 A true copy of order dated 22.10.2013 passed by the Ld. JMFC in Crl. Misc. Appln No.172 of 2013/C	273-274
16.	ANNEXURE:P-11 A true copy of order dated 22.10.2013 passed by the Ld. JMFC in Crl. Misc. Appln No.172 of 2013/C	275-276
17.	ANNEXURE:P-12 True copy of the W.P.No.10 of 2014 filed before the High Court of Judicature at Bombay Bench at Goa dated 21.12.2013	277-320
18.	ANNEXURE:P-13 A true copy of order dated 04.02.2014 passed by the High Court of Judicature at Bombay Bench at Goa in Cr. W. P. No.10 of 2014	321
19.	ANNEXURE:P-14 True copy of the letter dated 13.3.2014	322-326

20. ANNEXURE:P-15

A true copy of "Strategy Overview" dated Nil. 327-379

21. ANNEXURE:P-16

A true copy of "Data Protection and Security Guidelines for Registrars" dated nil. 380-397

22. ANNEXURE:P-17

True copy of the letter dated 13.3.2014 398-399

23. ANNEXURE:P-18

True copy of the letter dated 13.3.2014 400-401

24. ANNEXURE:P-19

A true copy of the Data Sharing Policy in use by UIDAI dated nil. 402-408

25. CRL.M.P.NO._____OF 2014

An application for Exemption from filing Certified Copy of Impugned Order 409-411

270

ANNEXURE P-9

IN THE HON'BLE COURT OF JUDICAL MAGISTRATE OF
FIRST CLASS
VASCO, GOA

CRL.Misc. Application NO.172 of 2013

IN

(RC 07(S)/2013-CBI/ACB/GOA)

Between
Central Bureau of Investigation,
Anticorruption Branch,
Goa. Complainant

V/s.

Unknown Male Person
& Others. Accused persons

Application filed by the investigation officer u/s. 91 Cr. P.C., for giving direction to the UIDAI for providing documents/ information to CBI.

May it please your Honour

It is respectfully submitted that, the investigation of above mentioned case was taken over by CBI, ACB, Goa on 11.09.2013, in pursuance of the Notification issued by Under Secretary (Home), Govt. of Goa u/s 6 of Delhi Special Police Establishment Act, 1946 vide No.27/20/2013-HD(G)/1829 dated 5.6.2013 and the subsequent Notifications of Govt. of India, signed by Under Secretary, DOPT vide No.228/45/2013-AVD-II both dated 20.8.2013 under sub section 5(1) r/w Sec 6 of

DSPE Act and u/s 3 of DSPE Act. The original FIR is submitted to this Hon'ble Court

The allegation as per the FIR, is that a seven year old girl student of Deepvihar Primary School, Vasco was raped inside the toilet of the school premises by an unknown male person during recess time, between 10.35 hrs to 10.50 hrs on 14.1.2013.

It is further submitted that the accused is still not apprehended and investigation is in progress During the course of investigation palm impression of an unknown person was obtained from the scene of crime in this regard it is proposed to obtain the data base of persons from Goa who had enrolled with the Unique Identification Authority of India (UIDAI) -i.e. Aadhar Card, which contains the finger prints also. This will enable the investigation for comparing the palm impressions available with UIDAI, with the palm impression obtained from the scene of crime.

It is submitted that as per the policy of UIDAI, directions from the Jurisdictional Court is required for parting with any information. Therefore the order of this Hon'ble Court is required for obtaining the data base of

persons from Goa, in soft copy/hard copy for comparing the same with the available data, to trace the accused in this case.

PRAYER

In view of above, it is humbly prayed that this Hon'ble Court may be pleased to issue orders to the Director general, UIDAI, New Delhi and the Dy. Director General, UIDAI, Technology Centre Bangalore for providing the data required for investigation by CBI.

Sd/-
(T.V. Joy)
Dy. Supdt. of Police
CBI, ACB, Goa.

Dated: 21/10/2013

Place: Goa.

//TRUE COPY//

ANNEXURE:P-10

IN THE HON'BLE COURT OF JUDICAL MAGISTRATE OF
FIRST CLASS VASCO, GOA

CRIMINAL MISC APPLN. NO. 172/2013/C

Between

Central Bureau of Investigation,
Anticorruption Branch, Goa.

Complainant

V/s.

Unknown Male Person
& Others.

Accused persons

To,

The Dy. Director General,
UIDAI, Technology Centre,
Bangalore

WHEREAS the above named complainant has filed is application before this Court praying that this Hon'ble Court may be pleased to issue orders to the Director General, UIDAI, New Delhi and the Dy. Director General, UIDAI, Technology Centre Bangalore for providing the data required for investigation by CBI.

AND WHEREAS after going through the said application this Court has passed the following order.

ORDER

As the information sought is important for further investigation in the case and also considering the nature

of the case, issue letter DG, UIDAI, New Delhi & DY. DG, UIDAI Technology Centre, Bangalore to provide the necessary data to the Dy. S.P. T.V. Joy, CBI, ACB, Goa.

Sd/-
22.10.13
I.M.R.F. Vasco

You are therefore, hereby directed to act accordingly as per the order of this Court.

Date this day of October, 2013.

Sd/-
(Sec. Prasbhudessai)
Judicial Magistrate First Class
Vasco Da Gama

//TRUE COPY//

275

ANNEXURE:P-11

CONFIDENTIAL/ BY HAND

C.B.I. GOA	Government of India Central Bureau of Investigation Anti- Corruption Brach-Goa Bungalow No. F-1, Type VI, GMC quarters, NH-17 Bambolim, Panaji Goa 403202, Phone 0832-2429971, 2469972, Fax2459974 e-mail hobacoa@cbi.gov.in

No.RC 7(S)/2013/CBI/ACB/Goa Dated: 23.10.2013

To,

The Deputy Director General
UIDAI, Technology Centre,
Bangalore

Sub: Investigation in RC7(S)2013/CBI/ACB/Goa,

pertaining to the sexual assault on a minor Girl

Student at Deepvihar Public School Vasco, Goa

Sir,

Kindly refer to the Order date d22.10.2013 issued by the Hon'ble Judicial Magistrate of First Class (JMFC), Vasco-da-Gama Goa, in Crl. Misc. Application No. 172/2013/C, Directing UIDAI to provide the information required in connection with the investigation of RC 7(S)/2013/CBI/ACB/Goa.

In this regard, it is requested that the data available in the data base of UIDAI, pertaining to the persons from the State of Goa, who had enrolled with the UIDAI (Adhar

Card) may be provided to the undersinged in Softcopy/ hardcopy for investigation purpose.

The original Order issued by the Hon'ble Court along with the copy of application submitted by the Investigation Officer is enclosed herewith.

Yours faithfully
Sd/-
(T.N. Joy)
Dy. Superintendent of Police
CBI, ACB, Goa

//TRUE COPY//

277

ANNEXURE P-12

IN THE HIGH COURT OF JUDICATURE AT BOMBAY,
BENCH AT GOA
CIVIL APPELLATE JURISDICTION
WRIT PETITION NO. 10 OF 2013

Unique Identification Authority of India & Anr.
....Petitioner(s)

VERSUS

Central Bureau of Investigation,
Anti Corruption Branch, Goa
....Respondent

INDEX

S. No.	Particulars	Page
1.	Proforma	
2.	Synopsis	A-G
3.	Writ Petition	1-27
4.	Exhibit A True copy of Criminal Application No-172/2013/C moved by Respondent before Judicial Magistrate.	28-29
5.	Exhibit B True copy of the order dated 22.10.2013 passed by Judicial Magistrate, First Class at Vasco Da Gama.	30
6.	Exhibit C True copy of letter dated 23.10.2013 Issued by Respondent.	31-34
7.	Vakalatnama	35-36

278

IN THE HIGH COURT OF JUDICATURE AT BOMBAY,
BENCH AT GOA
CIVIL APPELLATE JURISDICTION
WRIT PETITION NO. OF 2013

Unique Identification Authority of India & Anr.
....Petitioner(s)

VERSUS

Central Bureau of Investigation,
Anti Corruption Branch, Goa
....Respondent

SYNOPSIS & LIST Off DATES

S.NO	DATE	PARTICULARS
		The Petitioner, being the Unique Identification Authority of India ("UIDAI"), was constituted and notified by the Planning Commission on 28,01,2009 as an attached office under the aegis of Planning Commission with the responsibility of laying down plans and policies to Implement UIDAI scheme and is to own and operate the UIDAI database and further be responsible for its updation and maintenance on an ongoing basis. The Petitioner is

aggrieved by the order dated 22.10.2013 passed by Judicial Magistrate, First Class at Vasco Da Gama in Criminal Misc. Appln. No.172/2013/C wherein upon an application moved by the respondent, the Hon'ble Magistrate has directed the Petitioner Authority to provide the data available in its database Including biometrics (fingerprints) of all residents of Goa for Investigation of Case No, being RC 7(S)/2013/CBI/ACB/Goa pertaining to the sexual assault on a minor girl-student In Vasco, Goa, The aforesaid order passed by the ld. Magistrate is patently illegal, being violative of the provisions of Article 21 of the Constitution of India and is in further violation of the mandate given to UIDAI, which acts as a custodian of the data collected by it from the citizens, Furthermore the

said impugned order is in violation of UIDAI Policy on data sharing which has a clear mandate not to share data of any individual till the time the consent of the said person has not been obtained.

1.	28,01,2009	The Petitioner No.1 Authority came Into existence vide Notification No, Notification No-A-43011/02/2009-Admn. I dated 28.01.2009.
2.	22.10.2013	The Ld. Judicial Magistrate, First Class passed the Impugned ex-parte order dated 22.10.2013 wherein It was observed that since the Information sought was Important for further Investigation In the case and also considering the nature of the case, It directed DG, UIDAI, New Delhi and Dy, DG, UIDAI Technology Centre, Bangalore, to provide the necessary data to Respondent.

3.	23.10.2013	That pursuant to the aforesaid order, the Petitioner received a letter dated 23,10,2013 from the Deputy Superintendent of Police, CBI, Anti-Corruption Branch, Goa requesting it to provide data available in the data base of UIDAI, including fingerprints, of three persons whose name and address has been detailed in the said letter.
4.	December 2013	Aggrieved by the above-mentioned order, the Petitioners are constrained to approach this Hon'ble Court by way of the present Writ Petition for quashing and setting aside the order dated 22,10,2013 passed by the Ld, Judicial Magistrate, First Class.

II. <u>Points to be urged</u>

A) Whether the impugned Order is bad in law, being ex-fade illegal and violative of the provisions of Article 21 of the Constitution of India, which amongst the right to life and personal liberty, by its

Inherent nature, also Includes the Right to Privacy of a resident.

B) Whether the Impugned order further violates the provisions of Article 20(3) of the Constitution of India which provides protection against self-incrimination.

C) Whether the Impugned order is violative of Article 21, including the citizen's right to privacy, since as enshrined In Article 21, the said right can only be taken away as per procedure established by law.

D) Whether the Impugned order would not further violate Article 20(3) of the Constitution of India which affords protection to citizens against self-incrimination, in as much as the Article affords protection by providing that no person accused of any offence shall be compelled to be a witness against himself, By compulsorily directing the Petitioner Authority to provide data Including biometric data of the citizens of Goa, against their consent, or even knowledge, the Impugned order is clearly violative of Article 20(3), forcing the said persons to provide their fingerprints In a criminal

case which may be used as evidence against them at a subsequent stage.

E) Whether the Impugned order is beyond the scope of Section 91(1) of CrPC, wherein though, a Court or office-in-charge of a Police Station can Issue summons or a written order for the production of any document or any other thing necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under the code, the same has to be read with Section 124 of the Indian Evidence Act, 1872 read with Section 91(3) of the Cr.P.C, which clearly provides that provisions of the said section 91 shall not affect the provisions of Section 124 of the India Evidence Act which clearly provide that no public officer shall be compelled to disclose communications made to him In official confidence, when he considers that the public Interests would suffer by the disclosure.

F) Whether before passing the impugned order, the Ld, Judicial Magistrate ought not to have satisfied itself whether request for the specific data by Respondent

is being made after following the guidelines/ policies of UIDAI on data sharing.

G) Whether before passing the Impugned order, the Ld. Judicial Magistrate ought not to have considered the law as laid down by the Apex Court wherein right to privacy has held to be an integral part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution and once the facts in a given case constitute a right to privacy, Article 21 is attracted and the said right cannot be curtailed "except according to procedure established by law".

H) Whether vide the impugned order, the Ld, Judicial Magistrate could have directed Petitioner to supply information to the Respondents, which is voluntarily provided for by the residents, only for the purposes of maintaining a database and which is specifically to be used for implementation of various welfare schemes introduced by the Government.

I) Whether the Hon'ble Judicial Magistrate ought not to have passed the impugned order only after hearing the persons against whom such an order was being sought, since the said order has denied the

concerned Individuals their inherent right to file an appeal and challenge the said act of the respondent, being violative of their fundamental rights.

J) Whether the Hon'ble Judicial Magistrate ought not to have appreciated the fact that in the application filed before the ld. Judicial Magistrate, the Respondent had failed to produce any evidence/ documentation/ proof etc, on the basis of which it has demanded finger prints and instead have made a bald assertion that it proposes to obtain data base of all persons from Goa who had enrolled with the UIDAI.

K) Whether, while passing the Impugned order, the Ld. Judicial Magistrate ought to have appreciated the fact that the data base collected by the Petitioner is not for the convenience of Police or other investigative agencies but for implementation of Government's welfare schemes, in the course of investigation of a crime, if on the basis of inquiry, investigation and analysis, the police/ investigating authorities are able to zero in on suspects, then It has full mandate under the provisions of law to

demand data including finger prints from the accused and there is absolutely no requirement to approach the petitioner authority for the same.

L) Whether, while passing the Impugned order, the Ld, Judicial Magistrate ought to have appreciated the fact that that UIDAI does not collect biometric Information i.e. Iris scan and fingerprints, based on technologies, standards or procedures suitable for forensic purposes and therefore there is no saying on the potential forensic utility of the said resident information for criminal investigations or inquiries, thus, there is no mechanism with UIDAI of sharing the biometric information.

M) Whether the said impugned order passed by the Ld, Judicial magistrate, if not quashed and set aside, the same would create precedent wherein in each case of crime, the police/ investigative authorities would conveniently approach the petitioner authority for information/ data rather than investigating the case on its own facts and merits.

III. Acts and Rules;

1. The Constitution of India

--

2. The Code of Criminal Procedure, 1973

3. The Indian Evidence Act, 1872

4. Any other law/ Act which may be required.

Authorities;

To be cited at the time of hearing

Mumbai
Dated; 21st December 2013

Messrs. DSK Legal
Advocate for the petitioner

288

IN THE HIGH COURT OF JUDICATURE AT BOMBAY,
BENCH AT GOA

CIVIL APPELLATE JURISDICTION
WRIT PETITION NO. OF 2013

In the matter of Article 226 of the Constitution of India;

AND

In the matter of order dated 22.10.2013 passed by the Court of Judicial Magistrate, First Class at Vasco Da Gama In Criminal Misc, Appln. No-172/2013/C.

IN THE MATTER OF:

1. UNIQUE IDENTIFICATION AUTHORITY OF INDIA, Through Its Director General Having Headquarters at Planning Commission Government of India, 3rd Floor, Tower II Jeevan Bharati Building, Connaught Circus New Delhi - 110001.

2. Deputy Director-General, UIDAI Technology Centre, Bangalore. ....Petitioners

VERSUS

Central Bureau of Investigation, Anti-Corruption Branch, Goa.

TO,

THE HON'BLE CHIEF JUSTICE AND OTHER HON'BLE JUDGES OF THIS HON'BLE HIGH COURT OF JUDICATURE AT BOMBAY GOA BENCH

THE HUMBLE PETITION OP THE
PETITIONER'S ABOVE-NAMED

MOST RESPECTFULLY SHEWETH THAT:

1. The Petitioner, being the Unique Identification Authority of India ("UIDAI"), was constituted and notified by the Planning Commission on 28.01.2009 as an attached office under the aegis of Planning Commission. The UIDAI was given the responsibility to lay down plan and policies to Implement UIDAI scheme and shall own and operate the UIDAI database and be responsible for its updation and maintenance on an ongoing basis.

2. The Petitioner is aggrieved by the order dated 22.10.2013 passed by Judicial Magistrate, First Class at Vasco Da Gama in Criminal Misc. Appln. No.172/2013/C wherein upon an application moved by the Respondent, the Hon'ble Magistrate has directed the Petitioner Authority to provide the data available in its database including biometrics (fingerprints) of all residents of Goa for Investigation of Case No. being RC 7(S)/ 2013/ CBI/ ACB/Goa pertaining to the sexual assault on a minor girl-student in Vasco, Goa.

3. The aforesaid order passed by the Id. Magistrate is patently Illegal, being violative of the provisions of Article

--

21 of the Constitution of India and therefore liable to be set aside. The said Impugned order further violates the provisions of Article 20(3) of the Constitution of India in as much as the Article affords protection by providing that no person accused of any offence shall be compelled to be a witness against himself. By compulsorily directing the Petitioner Authority to provide data including biometric data of the citizens of Goa, against their consent, or even knowledge, the Impugned order is clearly violative of Article 20(3), forcing the said persons to provide their fingerprints in a criminal case which may be used as evidence against them at a subsequent stage.

4. Before going Into the facts and circumstances of the present case. It is pertinent to mention certain details about the Petitioner organization, the purpose of its establishment and the mandate and responsibility given to it:-

BACKGROUND OF AADHAR SCHEME

a. The UIDAI has been constituted by Notification No. A-43011/02/2009-Admn.I dated 28.01.2009 published in Part I, section 2 of the Gazette of India. It has been assigned responsibilities under the

Government of India (Allocation of Business Rules) in exercise of the powers conferred by Clause (3) of Article 77 of the Constitution, all issues relating to the Unique identification Authority of India including its organization, plans, policies programmes, schemes, funding and methodology to be adopted for achieving the objectives of the Authority are supervised by a duly constituted Cabinet Committee on Unique Identification Authority of India related issues. The Unique Identification Authority of India is bound by the General Financial Rules of the Government of India and is subject to audit by the Comptroller & Auditor General of India and is administered like any other Central Government department.

b. Aadhaar is a random 12-digit unique number which the UIDAI issues to all residents in India on a voluntary basis. The Aadhaar scheme is the unique identification project launched by the Government of India and is being implemented by the Unique Identification Authority of India (UIDAI), Aadhaar is simple and intuitive and designed for the common person to prove his identity using secure biometrics,

The simplicity of Aadhaar at the front/user end is complimented by a state of the art, fully secure, best in class back-end high technology.

c. The random number generated is devoid of any classification based on caste, creed, religion and geography. The number will be stored in a centralized database and linked to the basic demographics and biometric Information - photograph, ten fingerprints and Iris - of each Individual. It is verifiable in the form of Yes/ No to establish identity of a person in an online, cost-effective way. Further, to ensure uniqueness and privacy of the individual. It has been made essential that the bio-metrics captured are as per the specifications laid down by the Bio-metrics Standards Committee. In addition to biometrics, the UIDAI is collecting bare minimum demographic Information from the residents such as name, age, gender, address and relationship details in case of minors along with biometric information such as photograph, ten fingerprints and Iris for issue of unique identity number. It is pertinent to mention that in doing so the UIDAI is only computerizing the

age old system of Individuals providing name, address, age, gender, photo and fingerprints to Identify themselves. The use of biometrics/thumb impression is a time honored practice and Aadhaar is merely making a manual process electronic through computerization in a fully secure and foolproof manner. In UIDAI terminology this is commonly known as "Know your Resident (KYR)."

d. The partner registrars are using this resident Interface as an opportunity to update their own selected data bases such as ration card number, MGNREGS job card number, PAN card etc. This is commonly known as "Know your Resident Plus" (KYR+). Collection of these information is purely an initiative of respective State Registrars and not mandatory for issue of Aadhaar number. The UIDAI has executed Memoranda of Understanding (MoU) with the partners including all the States and Union Territories, financial institutions, PSUs etc, to act as Registrars for implementing the scheme. The Registrar General of India (RGI), authority under Ministry of Home Affairs conducting the exercise under National Population Register (NPR) is an

important partner registrar in the enrollment process.

e. The UIDAI scheme is envisaged as a means to enhance the delivery of welfare benefits and services, Before the advent of UID Scheme, there had been no single document which was uniformly acceptable as proof of identity across India - irrespective of age, gender and familial connections. Thus establishing identity had always been a challenge for the poor, particularly when they move from place to place. As a consequence, this lack of proof of Identity made it difficult for the poor to access benefits and services. In the absence of proofs of identity and residence, internal migrants were unable to claim social protection entitlements and remained excluded from government sponsored schemes and programmes, Aadhaar being an online identity, enrolling for UID Scheme Aadhaar number may be the first form of Identification they will have access to. This scheme has the potential to enable these migrants to obtain access to welfare services hitherto denied to them.

f. Enrolment of residents with proper verification is a key concern of the UIDAI and for this purpose it ensures proper verification of their demographic and biometric information. As a part of its pro-poor approach, the UIDAI focuses on enrolling India's poor and under privileged community for many of whom Aadhaar may be the first form of Identification, but no one gets enrolled for Aadhaar without undergoing the prescribed method of verification.

g. The Aadhaar number is a generic identity marker designed to enable multi-purpose functionalities. By intent it is not an ID in the nature of a Citizenship card or a functional domain specific ID like a Voter/Ration Card or a driving license all of which are commonly used as proxy ID documents In the absence of a pure ID like Aadhaar. Instead, Aadhaar is a generic proof of ID which can be used by agencies to Identify and authenticate Individual entitles (citizens, voters, Below Poverty Line, passport, pensioners, scholars etc) in their data base following their respective mandate and protocol.

h. The primary benefit of Aadhaar number is that by making for end to end computerization, Aadhaar will Increase transparency, accountability and audit as it will be possible to trace every benefit that flows from the Government to individual residents.

i. Presently, UIDAI undertakes following audits on a periodic basis; (i) Enrolment Client Audit; (ii) Enrolment Process (Field) Audits; (iii) ASDMSA Application Audits; (iv) Authentication User Agency Audits; (v) Data Center Audits; (vi) Security Audits; (vii) Impact Assessment (Grants In Aid for Research); and (viii) Other Third Party Audit Services.

J. The UID project is a complex technology project, Nowhere in the world such a large bio-metric database of a billion people is being maintained. The technical architecture of the UID scheme has been structured to ensure clear data verification, authentication and de-duplication, while ensuring a high level of privacy and information security. The Aadhaar scheme is the largest scheme in the world seeking to provide a unique Identification number to

more than one billion residents of India, As on 30th September 2013, more than 53 Crore residents have enrolled for Aadhaar and an amount of Rupees Three Thousand Four Hundred and Ninety Four Crore (Rs.3,494 crore) has been incurred on the programme by the Central Government, The Aadhaar scheme is primarily a developmental Initiative and its design features have been arrived at with the express purpose of Improving delivery of social security benefits and subsidies, plugging leakages and wastes, eliminating fakes and duplicates and enhancing transparency and accountability.

k. The introduction of Aadhaar needs to be seen in the same vein and as a part of the continuing quest of the Government to Improve efficient and transparent delivery of public services.

l. That it is submitted that UID scheme is not working under a legal vacuum. Even though the Cabinet has recently approved a legislative framework to replace National identification Authority of India (NIAI) Bill 2010, nevertheless, the IT Act and Rules made

thereunder are sufficient enough to regulate the collection, disclosure, and use of sensitive personal data In the form of biometric data or Information.

5. **BRIEF FACTS OF THE INSTANT PETITION:**

(i) Vide the notification dated 28.01.2009 the Unique Identification Authority of India was constituted. One of the primary roles of the UIDAI was to collect data from residents for the purposes of planning and implementing UIDAI scheme. The role that the Authority envisioned was to issue a unique Identification number (UIDAI) that could be verified and authenticated in an online, cost-effective manner, and which was robust enough to eliminate duplicate and fake identities. The authority was to further own and operate the UIDAI database and be responsible for its updation and maintenance on an ongoing basis.

(ii) Data is collected by the UIDAI in two parts, being:-

(a) Biometric Information - refers to either or both fingerprints and Iris scan Information stored by UIDAI in its Central Identities Data Repository (CIDR) located at Bangalore; and

(b) Demographic Information - which would include all other resident information including name, photograph, age, gender and address (that are necessarily required for a resident's enrollment in the Aadhar database) and also the resident's mobile number and e-mail Id (which are optional).

Resident information comprises of both biometric as well as demographic Information.

(iii) Pursuant to coming into existence, the UIDAI began the task of collecting information from residents all across the country. It is pertinent to mention here that UIDAI only acts as a custodian of resident information particularly biometric information which is voluntarily provided by the residents with a sole purpose of participating and getting benefits of Government welfare plans and schemes. Voluntarily providing the said information by the residents is with the inherent belief that such information database would be held by the Petitioner in official confidence and trust.

(iv) The Respondent, in its course of investigation of case no. RC 7(S)/2013/CBI/ACB/ Goa, pertaining to the sexual assault on a minor girl-student at a school in Vasco- Goa, filed an application u/s.91 of the Code of Criminal Procedure, 1973 ("CrPC") being Criminal Misc. Appln. No.172/2013/C praying for directions to the Director General of the Petitioner Authority and Dy. Director General, UIDAI, Technology Centre, Bangalore to provide data required for investigation by Respondent, being data available with UIDAI of all residents of Goa including fingerprints. A true copy of Criminal Misc, Application No.172/2013/C moved by Respondent is hereto annexed and marked as 'Exhibit A'.

(v) The Ld. Judicial Magistrate, First Class passed the impugned ex-parte order dated 22.10.2013 wherein it was observed that since the information sought was important for further investigation in the case and also considering the nature of the case. It directed DG, UIDAI, New Delhi and Dy, DG, UIDAI Technology Centre, Bangalore, to provide the necessary data to Respondent.

A true copy of the impugned Order dated 22.10.2013 passed by the Ld. Judicial Magistrate, First Class in Criminal Misc. Application No.172/2013/C is hereto annexed and marked as Exhibit B.

(vi) That pursuant to the aforesaid order, the Petitioner received a letter dated 23.10.2013 from the Deputy Superintendent of Police, CBI, Anti-Corruption Branch, Goa requesting it to provide data available in the data base of UIDAI. Including fingerprints, of three persons whose name and address has been detailed In the said letter.

A true copy of the said letter dated 23,10,2013 written by the Deputy Superintendent of Police, CBI, Anti-Corruption Branch, Goa addressed to the petitioner is hereto annexed and marked as Exhibit C.

(vii) Being aggrieved by the above-mentioned impugned Order dated 22.10.2013 the Petitioner is approaching the Hon'ble High Court under Article 226 of the Constitution of India on the following grounds which are without prejudice to each other.

302

6. **GROUNDS:**

A) That the impugned Order is bad in law being ex-fade illegal and violative of the provisions of Article 21 of the Constitution of India, which amongst the right to life and personal liberty, by its inherent nature, also includes the Right to Privacy of a resident. The said impugned order further violates the provisions of Article 20(3) of the Constitution of India which provides protection against self-incrimination.

B) That Article 21 of the Constitution of India clearly provides that no person shall be deprived of his life or personal liberty except for procedure established by law. In the context of the present case, the citizen's right to privacy, as enshrined in Article 21, can only be taken away as per procedure established by law. Since in this case, there exists no legislation that details the data sharing policy of UIDAI, procedure established would be the guidelines laid and policies of UIDAI (vide Government Notifications) which would provide the manner in which data so collected by UIDAI can be

shared with other agencies. Further Article 20(3) of the Constitution of India further affords protection to citizens against self-incrimination. In as much as the Article affords protection by providing that no person accused of any offence shall be compelled to be a witness against himself. By compulsorily directing the Petitioner Authority to provide data including biometric data of the citizens of Goa, against their consent, or even knowledge, the Impugned order is clearly violative of Article 20(3), forcing the said persons to provide their fingerprints in a criminal case which may be used as evidence against them at a subsequent stage.

C) That though under the provisions of Section 91(1) of Cr.P.C, a Court or office-in-charge of a Police Station can issue summons or a written order for the production of any document or any other thing necessary or desirable for the purposes of any Investigation, Inquiry, trial or other proceeding under the code, the same has to be read with Section 124 of the Indian Evidence Act, 1872 read with Section 91(3) of the Cr. PC, Section 91(3) Cr.PC clearly provides that provisions of the said

section 91 shall not affect the provisions of Section 124 of the India Evidence Act which clearly provide that no public officer shall be compelled to disclose communications made to him in official confidence, when he considers that the public interests would suffer by the disclosure. Hence reading the same in consonance with the scheme and policy of UIDAI, which has a strict mandate to share data only in such cases where the resident has given his/ her consent for sharing data, the said Impugned order, which forces the petitioner authority to provide data with regard to certain residents, without even their knowledge, let alone consent to the same, implies that it is clearly violative of the resident's right to privacy enshrined in Article 21 of the Constitution of India.

D) That in furtherance of procedure established by law, it is pertinent to note that the Petitioner Authority under the aegis of the Planning Commission has Issued an OM being No.4 (4)/57/134/2012-UIDAI/ROB dated 14.09.2012 which provides the framework/guidelines for Implementing the Data Sharing Policy of the UIDAI. The framework/

guidelines prescribed in the document are applicable to all State Governments or their Departments (hereinafter referred to as Requester) who are desirous of requesting for data from UIDAI for improving the delivery of benefits and services and cleansing their databases, Certain terms of the said OM are as follows;

"A, Data Sharing Mechanism

This section details the manner of sharing various types of data.

1. Demographic and Photo:

I. The demographic data and photo of residents who have given their consent for sharing of data can be shared using the same format as currently being used to share Aadhaar data with the Registrars, i.e., through EID-UID XML files. EID-UID XML files can be created for the required data and shared with the Requester using Secured File Transfer Protocol ("SFTP")/hard disk.

II. In case of any update in the data by the residents, UIDAI will provide the updated data to the agencies

with, whom UIDAI shared the data initially, provided resident consent is available for data sharing. The format of data sharing will be the same as described above.

III. Shared data should be secured using following multi-layer security approach:

a. EID-UID XML files would be encrypted with public key provided by the requester.

b. Point to point connection and IP based restrictions would be implemented for SFTP access to ensure that the data can be downloaded from an authorized location only.

2. Biometrics Data

a. Biometrics shall not be shared by default, Sharing shall be limited to minimum and specific biometric data required for fulfilling the objectives of the Department concerned.

b. Raw biometric Images shall not be ordinarily shared.

c. Only templates in ISO form shall be shared. The template have smaller packet size, requiring

lesser space for Requester Department for storage and support open standard adoption even for card based schemes.

d. Templates can be taken from authentication system to create a UID-FMR mapping file. The file would be encrypted with public key of the Requester and signed.

e. Biometric data would be shared in an offline manner using a physical media. After copying the data in a secured location, the requester is required to delete the data from physical media used for sharing, including physical destruction of the media in such a manner that data can not be recovered from media."

E) Furthermore vide D.O letter dated 11.09.2013 the Director General and Mission Director of UIDAI clarified as under:

"1. Mandate of Unique Identification Authority of India (UIDAI) is to give Unique Identity Number called Aadhaar, to the residents of India. This is done on the basis of demographic (Name, Gender, DoB, Address) and biometric (Photo, 10 finger

--

prints, 2 iris scan) information collected from each resident. The biometric Information (10 finger prints, 2 iris scan) is de-duplicated with information pertaining to other Aadhaar number holders available in UIDAI's Central ID Data Repository (CIDR), on a 1:N matching basis.

2. UIDAI mandate does not allow for any Instance of 1:N matching, except for the generation of Aadhaar number where the biometric information has been collected in accordance with the laid down procedure.

3. All authentications are done on a 1:1 basis for which it is necessary to have Aadhaar number of an individual and his other details including biometric information for matching and verification. As a corollary, Authentication cannot be processed in any case where either Aadhaar Number is not available or where Aadhaar number is available but other details are not available.

4. In the event that both Aadhaar number and other details are available, the process of Authentication is feasible, provided one of the following conditions is met:

a. Authentication request is routed through existing Authentication User Agency (AUA) or Authentication Service Agency (ASA) with explicit consent of resident, in writing or electronically authenticated.

b. Request is received as a direction /order of competent court.

c. Request is received on grounds of national security from Central Government Ministry/Department with the approval of an officer not below the rank of a Joint Secretary,"

F) Thus, perusal of the afore-mentioned provisions would make it amply clear that none of the procedure established/ requirements enunciated In the afore-mentioned clarification have been compiled with by the Respondent in making a request for the said data base from the Petitioner Authority and instead the Respondent has merely requested for data for certain Individuals vide its letter dated 23.10.2013. The Petitioner's policy makes it mandatory for permission to be obtained from the concerned person whose data is being sought and only in case where such permission is

granted can the Petitioner authority part with such data.

G) That in the present case, before passing the impugned order, the Ld. Judicial Magistrate ought to have satisfied itself whether request for the specific data by Respondent is being made after following the guidelines/policies of UIDAI on data sharing. However, in complete derogation of such an assumption and satisfaction, the Ld. Magistrate went ahead to pass the Impugned order merely on the asking of the respondent without even granting an opportunity of hearing either to the persons whose records were being demanded or to the Petitioner Authority.

H) That the Hon'ble Supreme Court in People's Union for Civil Liberties v. Union of India & Ors. [(1997) 1 SCC 301] have categorically held, "We have, therefore, no hesitation in holding that right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution, Once the facts in a given case constitute a right to privacy, Article 21 is attracted,

The said right cannot be curtailed "except according to procedure established by law".

i) That it is further an established principle of law, as laid down by the Hon'ble Supreme Court in a plethora of Judgments, that any legislation that intrudes on the personal liberty of a resident, must, in order to be termed constitutional, satisfy the triple test as laid down by the Hon'ble Supreme Court in Maneka Gandhi v. Union of India. The said triple test which is required of any law intruding personal liberty of residents under Articles 21 are:

I. a procedure must be prescribed for the same;

I) The procedure must withstand the test of one or more of the fundamental rights conferred under Article 19 which may be applicable in a given situation.

II) It must also be liable to be tested with reference to Article 14.

In the afore-mentioned case, the privacy of a resident's financial records maintained by bank as a trustee were discussed and the Hon'ble Supreme

Court had mentioned that the above 3 tests need to be applied before any details of mortgage or other financial transactions can be shared with any agency, On the similar grounds, the UIDAI is a trustee of resident's Demographic and Biometric data and before sharing of resident's data the triple test need to be applied.

J) That the Hon'ble Supreme Court further, in Smt Selvi & Ors, v. State of Karnataka [(2010) 7 SCC 263] wherein the constitutional validity of administration of Narcoanalysis, polygraph examination and the Brain Electrical Activation Profile (BEAP). was considered, held that subjecting a person to the impugned techniques in an involuntary manner violates the prescribed boundaries of privacy. The Court in fact further held that compulsory administration of the said techniques constitutes 'cruel, inhuman or degrading treatment' in the context of Article 21. Thus in this regard the law stands clear that Involuntary techniques to collect data would squarely be Invasion and violation of the fundamental rights granted to the citizens under Article 21.

K) That the Petitioner collects the information from resident, which is voluntarily provided for, only for the purposes of maintaining a database which would be specifically used for implementation of various welfare schemes introduced by the Government. At the time when the said information is provided to UIDAI authorities, every resident is entitled to have the opportunity to consent regarding further sharing of their information by UIDAI specifically for improvement of delivery of welfare and public services or for the provisioning of certain banking facilities. When a resident has not granted his/ her consent for sharing of their data for any other purpose, UIDAI would be in complete derogation of its mandate in passing such data to a third party including Investigation agencies of the State and in fact would become an active. accomplice in violating this fundamental right of privacy of residents.

L) That had the petitioner authority known that the data base being collected and maintained by it could also be used for investigative purposes, the said fact would have been disclosed to the concerned persons

by the petitioner at the time of providing of the said data or not.

M) That the Hon'ble Judicial Magistrate ought not to have passed the impugned order without hearing the persons against whom such an order was being sought, since the said order has denied the concerned individuals their inherent right to file an appeal and challenge the said act of the respondent, being violative of their fundamental rights.

N) That in the application filed before the ld. Judicial Magistrate, the Respondent has failed to produce any evidence/ documentation/proof etc, on the basis of which it has demanded finger prints and instead have made a bald assertion that it proposes to obtain data base of all persons from Goa who had enrolled with the UIDAI including fingerprints as this will enable the investigation, by comparing the palm impressions available with UIDAI with the palm impressions obtained from the crime scene. It is respectfully submitted that UIDAI has collected biometric information of lakhs of residents residing in the State of Goa and it is not possible for the

Petitioner authority to keep on filtering its data base to provide information as and when demanded by the Police/other Investigation authorities. Furthermore, it is submitted that UIDAI cannot give data of fingerprints; it can only authenticate the Biometrics of the residents. It is respectfully submitted that the database of residents of Goa with UIDAI is approximately 12 Lacs and sharing the whole database would amount to violation of Rights of Privacy of the individuals of Goa under Article 20(3) and 21 of the Constitution of India, as well as rights accorded by Section 91(3) of the CrPC as well as provisions of Identification of Prisoners Act, 1920.

O) That while passing the impugned order, the Ld. Judicial Magistrate ought to have appreciated the fact that the data base collected by the Petitioner is not for the convenience of Police or other investigative agencies but for implementation of Government's welfare schemes. In the course of investigation of a crime, if on the basis of inquiry, investigation and analysis, the police/investigating authorities are able to zero in on suspects, then it has full mandate under the provisions of law to

demand data including finger prints from the accused and there is absolutely no requirement to approach the petitioner authority for the same.

P) That in this regard it is pertinent to mention here that UIDAI does not collect biometric information i.e. iris scan and fingerprints, based on technologies, standards or procedures suitable for forensic purposes and therefore there is no saying on the potential forensic utility of the said resident information for criminal investigations or inquiries, Thus, there is no mechanism with UIDAI of sharing the biometric information.

Q) That if the said impugned order passed by the Ld. Judicial magistrate is not quashed and set aside, the same would create precedent wherein in each case of crime, the police/ investigative authorities would conveniently approach the petitioner authority for information/ data rather than investigating the case on its own facts and merits. Further there is also no saying if the said data could be misused by any person in whose possession it is handed.

R) In the facts and circumstances as above-mentioned as also the grounds mentioned herein, the Impugned order is thus perverse and liable to be quashed and set aside.

7. In the aforesaid circumstances, the Petitioner respectfully says and submits that this Hon'ble Court be pleased to issue any appropriate writ, order or direction, calling for the papers and proceedings leading to the passing of the impugned Order dated 22.10.2013 passed by the Ld. Judicial Magistrate, First Class at Vasco da Gama and after going into the legality, validity and propriety thereof, to quash and/ or set aside the same.

8. The Petitioner submits that the impugned Order is patently illegal and ex-fade unconstitutional. The balance of convenience is in favour of the Petitioner. Grave and irreparable loss, harm and injury shall be caused to the petitioner in the event the impugned Order is not stayed. The Petitioner therefore, says and submit that pending the hearing and final disposal of the writ petition, this Hon'ble Court be pleased to stay the operation of the impugned Order dated 22.10.2013 passed by the Ld. Judicial Magistrate, First Class at Vasco da Gama.

9. The Petitioner states that other than this Petition no other Petition/ application/ suit or proceedings pertaining to the subject matter of this petition has been/ was filed by it either in the Hon'ble Supreme Court of India. In this Hon'ble Court. In any other Hon'ble Court or any other forum (judicial, quasi-Judicial or administrative).

10. The Respondent has its offices within the Jurisdiction of this Hon'ble Court and the cause of action has also arisen within the jurisdiction of this Hon'ble Court. Therefore, this Hon'ble Court has Jurisdiction to entertain this Petition.

11. The Petitioner has no other equally efficacious or alternative remedy and the relief's prayed for, if granted, would be complete.

12. The Petitioner has paid the requisite court fees of Rs.....

13. The Petitioner therefore PRAYS:-

a) That this Hon'ble Court be pleased to issue any appropriate writ, order or direction, calling for the papers and proceedings leading to the passing of the impugned order dated 22.10.2013 passed by

the Ld. Judicial Magistrate, First Class at Vasco da Gama being Exhibit A hereto and to quash and / or set aside the same.

b) That pending the hearing and final disposal of the writ petition this Hon'ble Court be pleased to stay the effect, operation and implementation of the impugned order dated 22.10.2013 passed by the Ld, Judicial Magistrate, First Class at Vasco da Gama being Exhibit A hereto;

c) For ad-Interim reliefs in the prayer clause (b) above;

d) For costs of this Writ Petition be provided.

e) For such other and further orders as this Hon'ble Court may deem fit and proper in the nature and circumstances of the case.

AND FOR THIS ACT OF KINDNESS AND JUSTICE, THE PETITIONERS AS IN THE DUTY BOUND SHALL EVER PRAY.

Solemnly affirmed at Mumbai
On this 21st day of December 2013

Before me,

Advocate for the Petitioner

320

VERIFICATION

I, Surya Krishnamurthy, Deputy Director of the Petitioner Authority at the Regional Office, Mumbai and having my office at UIDAI Regional Office, 7th Floor, MTNL Building, Cuffe Parade, Mumbai 400 004, do hereby solemnly declare and state that what is stated in paragraphs 1 to 5 s true to my own knowledge and what is stated in the remainder paragraphs is stated on information and belief and I believe the same to be true.

Solemnly affirmed at Mumbai
On this 21st day of December 2013

Before me

Advocates for the Petitioner
M/s. DSK Legal

//TRUE COPY//

ANNEXURE P-13

IN THE HIGH COURT OF BOMBAY AT GOA
CRIMINAL WRIT PETITION NO. 10 OF 2014

UNIQUE IDENTIFICATION AUTHORITY OF INDIA
THROUGH ITS DIRECTOR GENERAL AND ANR.
Petitioners

Versus

CENTRAL BUREAU OF INVESTIGATION Respondent

Mr. Ravi Prakash, Ms. Volita Singh and Mr. Hanumant D. Naik, Advocate for the petitioners.

Coram: SMT. R.S. DALVI &
F.M. REIS. JJ.

Date:- 4th February, 2014

P.C.:-

Leave to amend granted to add the State as party respondent. The amendment to be carried out within a period of one week.

2. Issue notice upon the present respondent, as also the newly added respondent, returnable on 18th February 2014. Humdust allowed. The petitioners may serve by private service also.

3. In the meantime, the impugned order of the learned Judicial Magistrate, First Class, Vasco da Gama dated 22nd October, 2013 shall not be acted upon for two Weeks.

F.M. REIS, J. SMT. R.S: DALVI, J

//true copy//

322
ANNEXURE-7

DSK Legal
True Value, True Values

DSK Legal
Advocates & Solicitors
4, Aradhana Enclave
R.KPuram, Sector 13
Opposite Hotel Hyatt
New Delhi-110 066
India

T:+911166616666
F:+911166616600

13.03.2014

Dear Sir

Ref: UIDAI & Anr. v. CBI - Goa & Anr. Writ Petition (Cr.) No.10 of 2014 before the Hon'ble High Court of Bombay at Goa

With respect to the captioned Writ Petition, as you would be aware, we submitted our rejoinder - affidavit dated 24.02.2014 on the same date before the Hon'ble High Court wherein the following submissions were made by us:

- That it is humbly submitted that the request of the respondent no.1 in demanding from the petitioner to compare chance finger prints with the biometric data already available is not only legally untenable on the yardstick of constitutional safeguards and beyond the mandate of the petitioner authority, but the same is also technically not possible given the current software implementation. UIDAI system is designed and built to de-duplicate biometrics of enrolled residents using 10 fingerprints, 2 irises, and

I facial image captured on a computer client machine specially designed and developed by UIDAI called 'Aadhhar Enrolment Client' with extensive quality and compliance checks. De-duplication requires multi-modal (including ten finger prints, two irises and face) fusion scoring. Searching entire database using a few partial fingerprints that too latent prints having moderate/poor quality or quality specifications not matching -with those captured at UIDAI's Aadhaar Enrolment Client machines, could potentially produce lakhs of false matches due to its fundamental nature. This means any such random search, which is now being demanded by the Respondent No.1, even if implemented in the current system, will put lakhs of innocent people under the scanner.

- That the current system, including de-duplication sub-system, has functional capability to de-duplicate only from the biometric images of created using Aadhaar Enrolment Client. This means that to search using latent/ chance fingerprints on a disc several parts of the current Aadhaar system need to be changed, re-designed, re-built, and entire de-

duplication system re-tuned and expanded to include forensic search features. Building a system that can search using latent fingerprints, quite like criminal database searches, is not within the constitutional and legal mandate and scope of UIDAI and fundamentally against the core reason residents have provided their data voluntarily to UDIAI.

While submissions were again being made on the above-mentioned proposition on 26.02.2014 wherein the counsel for the petitioner categorically stated that the current software technology/ systems in place does not permit/ makes it impossible for the petitioner to compare chance fingerprints. To this the Ld. Advocate General immediately retorted that we were trying to mislead the Court and that even the Police/ CBI with their limited data-base could carry out such a comparison. To counter the said averment counsel for the petitioner even submitted that being a Government instrumentality and having placed an affidavit on record in this regard, we could not possibly be misleading the Court. To this the Advocate General again retorted to have this claim of UIDAI verified, upon which the petitioner's counsel asked the Court to please do the same. The same was however

said to counter the contention made by State that we were providing incorrect information. Furthermore when the Ld. Advocate General requested and suggested the name of Director General, CFSL to appoint an expert to verify the petitioner's claim, at that point of time also it was submitted by the counsel for the petitioner that CFSL is a body concerned with forensics and they would not be able to test the compatibility of the petitioner's "software" in any manner and the same needs to be carried out by an expert who is proficient in the said field of software technology.

When the Court accepted the request of the Ld, Advocate General, it was at that time that the counsel for the petitioner sought instructions from DDG and to counter the stand of State of Goa in appointing an expert, sought an expert to be appointed from UIDAI's side also who could furnish a report.

However vide the interim order dated 26.02.2014, incorrectly stating the submission of the petitioner, the High Court erroneously observed that petitioner had agreed to test the competence of its data base (instead of software/ current technology/ systems in place) in

comparing chance finger prints given in electronic form with the data base of the petitioner. The Court further directed Director-General, Central Forensic and Scientific Laboratory (CFSL), New Delhi to appoint an expert to ascertain from the petitioner's data base whether the data base of the petitioner has the technological capability for matching the chance fingerprints electronically obtained with its data base. The Petitioner was also given the opportunity to obtain a report from any expert deemed fit by the petitioner. Report of both the experts was directed to filed within two weeks. Further the Court held that the legal aspect of right to information and right to privacy would be considered by it subject to the ultimate decision of this Hon'ble Court in Justice K.S. Puttaswamy. v UOI (Writ Petition (C) No.494/2012) which is still pending.

This is for your information & record.

Sd/-
(RAVI PRAKASH)

//TRUE COPY//

327
ANN-P-15

UIDAI STRATEGY OVERVIEW

CREATING A UNIQUE IDENTITY NUMBER FOR EVERY RESIDENT IN INDIA

Unique Identification Authority of India (UIDAI)

Planning Commission, Govt. of India

April, 2010

CONTENTS

Executive Summary 1
1 Introduction and historical background 6
2 The UIDAI implementation model 10
3 Enrolment into the UID system 14
4 Ensuring strong authentication and what it means for the UIDAI 25
5 Legal framework 30
6 Data security and fraud 33
7 Technology architecture of the UIDAI 35
8 Project execution 37
9 Project risks 38
10 UID-enabled micropayment architecture 39
1.1 Historical background and evolution of the UIDAI project..... 6
1.2 The UIDAI Approach 9
2.1 The Central Identities Data Repository (CIDR) 10
2.2 The Unique Identity Number 10
2.3 The Unique ID agencies. 11
2.4 Setting standards on demographic data and biometrics 12
3.1 The enrolment process 14
3.2 Enrolment strategy in rural and urban India 16
3.3 A focused effort to enroll the poor and hard to reach groups 17
3.4 Enrolment cost 19
3.5 Ensuring clean enrolment data from registrars 20
3.6 Updating UID details 20
3.7 Reaching critical mass in enrolments 21
3.8 Tracking enrolments across the country 22
3.9 Reaching a sustainable steady state in enrolments 23
4.1 Enabling UID adoption for authentication 25
4.2 Types of authentication 26
4.3 Authentication and the UIDAI revenue model 27
6.1 Protecting personal information of residents 33
6.2 Fraud scenarios 34
7.1 System architecture 35
8.1 Addressing challenges of scale 37
10.1 Features of UID-enabled micropayments 40
10.2 Benefits 41
10.3 Conclusion

328

Executive Summary

Overview

In India, an inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies. Public as well as private sector agencies across the country typically require proof of identity before providing individuals with services. But till date, there remains no nationally accepted, verified identity number that both residents and agencies can use with ease and confidence.

As a result, every time an individual tries to access a benefit or service, they must undergo a full cycle of identity verification. Different service providers also often have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual.

Such duplication of effort and 'identity silos' increase overall costs of identification, and cause extreme inconvenience to the individual. This approach is especially unfair to India's poor and under privileged residents, who usually lack identity documentation, and find it difficult to meet the costs of multiple verification processes.

There are clearly, immense benefits from a mechanism that uniquely identifies a person, and ensures instant identity verification. The need to prove identity only once will bring down Transaction costs for the poor. A clear identity number would also transform the delivery of social welfare programs by making them more inclusive of communities now cut off from such benefits due to their lack of identification. It would enable the government to shift from indirect to direct Benefits, and help verify whether the intended beneficiaries actually receive funds/subsidies.

A single, universal identity number will also be transformational in eliminating fraud and duplicate identities, since individuals will no longer be able to represent

Themselves differently to different agencies. This will result in significant savings to the state exchequer.

The UIDAI –evolving an approach to identity

The Government of India undertook an effort to provide a clear identity to residents first in 1993, with the issue of photo identity cards by the Election Commission. Subsequently in 2003, the Government approved the Multipurpose National Identity Card(MNIC).

The Unique Identification Authority of India (UIDAI) was established in January 2009, as an attached office to the Planning Commission. The purpose of the UIDAI is to issue a unique identification number (UID) to all Indian residents that is (a) robust enough to eliminate duplicate and fake identities, and (b) can be verified and authenticated in an easy, cost-effective way. The UIDAI's approach will keep in mind the learnings from the government's previous efforts at issuing identity.

The UIDAI will be created as a statutory body under a separate legislation to fulfill its objectives. The law will also stipulate rules, regulations, processes and protocols to be followed by different agencies partnering with the UIDAI in issuing and verifying unique identity numbers.

The UIDAI will be created as a statutory body under a separate legislation to fulfill its objectives. The law will also stipulate rules, regulations, processes and protocols to be followed by different agencies partnering with the UIDAI in issuing and verifying unique identity numbers.

Features of the UIDAI model

The Unique Identification number (UID) will only provide identity: The UIDAI's purview will be limited to the issue of unique identification numbers linked to a person's demographic and biometric information. The UID will only guarantee identity, not rights, benefits or entitlements.

The UID will prove identity, not citizenship: All residents in the country can be issued a unique ID. The UID is proof of identity and does not confer citizenship.

A pro-poor approach: The UIDAI envisions full enrolment of residents, with a focus on enrolling India's poor and underprivileged communities. The Registrars that the UIDAI plans to partner with – the NREGA, RSBY, and PDS – will help bring large numbers of the poor and under privileged into the UID system. The UID method of authentication will also improve service delivery for the poor.

Enrolment of residents with proper verification: Existing identity databases in India are fraught with problems of fraud and duplicate/ghost beneficiaries. To prevent this from seeping into the UIDAI database, the UIDAI plans to enrol residents into its database with proper verification of their demographic and

biometric information. This will ensure that the data collected is clean from the start of the program.

However, much of the poor and underserved population lack identity documents and the UID may be the first form of identification they have access to. The UIDAI will ensure that the Know Your Resident (KYR) standards don't become a barrier for enrolling the poor, and will devise suitable procedures to ensure their inclusion without compromising the integrity of the data.

A partnership model: The UIDAI approach leverages the existing infrastructure of government and private agencies across India. The UIDAI will be the regulatory authority managing a Central Identities Data Repository (CIDR), which will issue UIDs, update resident information, and authenticate the identity of residents as required.

In addition, the UIDAI will partner with agencies such as central and state departments and private sector agencies who will be 'Registrars' for the UIDAI. Registrars will process UID applications, and connect to the CIDR to de-duplicate resident information and receive UID numbers. These Registrars can either be enrollers, or will appoint agencies as enrollers, who will interface with people seeking UID numbers. The Authority will also partner with service providers for authentication.

The UIDAI will emphasize a flexible model for Registrars: The Registrars will retain significant flexibility in their processes, including issuing cards, pricing, expanding KYR (Know Your Resident) verification, collecting demographic data on residents for their specific requirements, and in authentication. The UIDAI will

provide standards to enable Registrars maintain uniformity in collecting certain demographic and biometric information, and in basic KYR. These standards have been finalized by the Demographic Data Standards and Verification Procedures Committee and Biometric Standards Committees which was constituted by the UIDAI constituted.

Enrolment will not be mandated: The UIDAI approach will be a demand-driven one, where the benefits and services that are linked to the UID will ensure demand for the number. This will not however, preclude governments or Registrars from mandating enrolment.

The UIDAI's role is limited to issuing the number. This number may be printed on the document/card that is issued by the Registrar. Loading intelligence into identity numbers makes Them susceptible to fraud and theft. The UID will be a random number.

The UIDAI will seek the Following demographic and biometric information in order to issue a UID number:

Name

Date of birth

Gender

Father's/Husband's/ Guardian's name and UID number(optional for adult residents)

Mother's/ Wife's/ Guardian's name and UID number(optional for adult residents)

Introducer's name and UID number(in case of lack of documents)

Address

All ten fingerprints, photograph and both iris scans

Registrars will send the applicant's data to the CIDR for deduplication.

- The CIDR will perform a search on key demographic fields and on the biometrics for each new enrolment, to ensure that no duplicates exist.

The incentives in the UID system are aligned towards a self-cleaning mechanism.

The existing patchwork of multiple databases in India gives individuals the incentive to provide different personal information to different agencies. Since de-duplication in the UID system ensures that residents have only one chance to be in the database, individuals will provide accurate data. This incentive will be come especially powerful as benefits and entitlements are linked to the UID.

- The UIDAI will offer a strong form of online authentication, where agencies can compare demographic and biometric information of the resident with the record stored in the central database. The Authority will support Registrars and agencies in adopting the UID authentication process ,and will help define the infrastructure and processes they need.

Enrolment will not be mandated:

The UIDAI will issue a number, not a card:

The number will not contain intelligence:

The UIDAI will only collect basic information on the resident:

Process to ensure no duplicates:

- Online authentication:

The UIDAI will not share resident data:

Technology will undergird the UIDAI system:

For residents:

For Registrars and enrollers:

For Governments:

- The UIDAI envisions a balance between 'privacy and purpose' when it comes to the information it collects on residents. The agencies may store the information of residents they enrol if they are authorized to do so, but they will not have access to the information in the UID database. The UIDAI will answer requests to authenticate identity only through a 'Yes' or 'No' response

Technology systems will have a major role across the UIDAI infrastructure. The UID database will be stored on a central server. Enrolment of the resident will be computerized, and information exchange between Registrars and the CIDR will be over a network. Authentication of the resident will be online. The Authority will also put systems in place for the security and safety of information.

The UID will become the single source of identity verification. Once residents enrol, they can use the number multiple times – they would be spared the hassle of repeatedly providing supporting identity documents each time they wish to access services such as obtaining a bank account, passport, driving license, and so on. By providing a clear proof of identity, the UID will also facilitate entry for poor and underprivileged residents into the formal banking system, and the opportunity to avail services provided by the government and the private sector. The UID will also give migrants mobility of identity.

- The UIDAI will only enrol residents after de-duplicating their records. This will help Registrars clean out duplicates from their databases, enabling significant efficiencies and cost savings. For Registrars focused on cost, the UIDAI's verification processes will ensure lower KYR costs. For Registrars focused on social goals, a reliable identification number will enable them to broaden their reach into groups that till now, have been difficult to authenticate. The strong authentication that the UID number offers will improve services, leading to better resident satisfaction.

Eliminating duplication under various schemes is expected to save substantial

money for the government exchequer. It will also provide governments with accurate data on residents, enable direct benefit programs, and allow government departments to coordinate investments and share information.

By providing identity authentication, the UIDAI will be taking on a process that costs agencies and service providers hundreds of crores every year. The Authority will evolve suitable policies on the issue of charging a fee for its authentication services, which will offset its long-term costs.

Registrars and service providers will also be able to charge for the cards they issue residents with the UID number. Such pricing will be within UIDAI guidelines.

Benefits

Revenue Model

Timelines

Conclusion

The UIDAI will start issuing UIDs between August 2010 and February 2011, and plans to cover 600million people within 4 years from the start of the issuing of the first set of UIDs. This can be accelerated if more Registrars partner with the UIDAI for both enrolment and authentication. The adoption of UIDs is expected to gain momentum with time, as the number establishes itself as the most accepted identity proof in the country. India will be the first country to implement a biometric-based unique ID system for its residents on such a large scale. The UID will serve as a universal proof of identity, allowing residents to prove their identity anywhere in the country. It will give the government a clear view of India's population, enabling it to target and deliver services effectively, achieve greater returns on social investments ,and monitor money and resource flows across the country. The timing of this initiative is encouraging – the creation of the UIDAI coincides with growing social investment in India, a shift in focus to direct benefits, and with the spread of IT and mobile phones, which has made the public receptive to

technology-based solutions. The UIDAI is committed to making this project a success. An initiative of this magnitude will also require the active participation of central, state and local governments, as well as public and private sector agencies across the country. With their support, the project will help realize a larger vision of inclusion and development for India.

Unique Identification Authority of India

Introduction and historical background

A crucial factor that determines an individual' swell-being in a country is whether their identity is recognized in the eyes of the government. Weak identity limits the power of the country's residents when it comes to claiming basic political and economic rights. The lack of identity is especially detrimental for the poor and the underprivileged, the people who live in India's "social, political and economic periphery". Agencies in both the public and private sector in India usually require a clear proof of identity to provide services. Since the poor often lack such documentation, they face enormous barriers in accessing benefits and subsidies. For governments and individuals alike, strong identity for residents has real economic value. While weak identity systems cause the individual to miss out on benefits and services, it also makes it difficult for the government to account for money and resource flows across a country. In addition, it complicates government efforts to account for residents during emergencies and security threats.

However in India, the goal of issuing a universally used, unique identity number to each resident poses a significant challenge .A project of this scale has not been attempted anywhere in the world, and requires an innovative model, distinct from what we have witnessed in identity systems so far anywhere in the world.

The Unique identification project was initially conceived by the Planning Commission as an initiative that would provide a clear and unique identity number.

for each resident across the country and would be used primarily as the basis for efficient delivery of welfare services. It would also act as a tool for effective monitoring of various programs and schemes of the Government.

The concept of unique identification was first discussed and worked upon since 2006 when administrative approval for the project –"Unique ID for BPL families" was given on March 3rd, 2006by the Department of Information Technology, Ministry of Communications and Information Technology. This project was to be implemented by the NIC over a period of 12 months.

Subsequently, a Processes Committee to suggest processes for updation, modification, addition and deletion of data fields from the core data base to be created under the Unique ID for BPL families Project was set upon July 3rd, 2006. A "Strategic Vision on the UID Project" was prepared and submitted to this Committee. It envisaged the close linkage that the UID would have to the electoral database. The Committee also appreciated the need of a UID Authority to be created by an executive order under the aegis of the Planning Commission to ensure a pan-departmental and neutral identity for the Authority and at the same time enable a focused approach to attaining the goals set for the XI Plan. The Seventh

1.1 Historicalbackgroundandevolution of theUIDAIproject

Meeting of the Process Committee on 30th August 2007 decided to furnish to the Planning Commission a detailed proposal based on the resource model for seeking its "in principle" approval. At the same time, the Registrar General of India was engaged in the creation of the National Population Registrar and issuance of Multi-purpose National Identity Cards to citizens of India. Therefore, it was decided, with the approval of the Prime Minister, to constitute an Empowered

Group of Ministers (EGoM) to collate the two schemes – the National Population Register under the Citizenship Act, 1955 and the Unique Identification Number project of the Department of Information Technology. The EGoM was also empowered to look into the methodology and specific milestones for early and effective completion of the Project and take a final view on these.

TheEGoMwas constitutedonDecember4th, 2006. The was held on November 27th, 2007. It recognised the need for creating an identity related resident database, regardless of whether the database is created based on a de-novo collection of individual data or is based on already existing data such as the voter list. It also recognised that there is a crucial and imperative need to identify and establish an institutional mechanism that will "own" the database and will be responsible for its maintenance and updating on an ongoing basis, post its creation.

The was held on January 28th, 2008. It decided on the strategy for the collation ofNPRandUID. Inter-alia, the proposal to establishUIDAuthority under the Planning Commission was approved.

The was held on August 7th, 2008. The Planning Commission had placed before the EGoM a detailed proposal for setting up the UIDAI. The meeting decided that certain issues raised by the members with relation to the UIDAI would need to be examined by an official level committee. It referred the matter to a Committee of Secretaries to examine and give its recommendations to the EGoM to facilitate a final decision.

Subsequent to the Committee of Secretaries recommendations, the was held on November 4th, 2008.The recommendations of the Committee of Secretaries was presented to the EGoM and the following decisions were taken:

a) Initially the UIDAI may be notified as an executive authority, and investing it with statutory authority could be taken up for consideration later at an appropriate time.

b) UIDAI may limit its activities to the creation of the initial database from the electoral roll/EPIC data. UIDAI may however additionally issue instructions to agencies that undertake creation of databases to ensure standardization of data elements.

c) UIDAI will take its own decision as to how to build the database.

d) UIDAI would be anchored in the Planning Commission for five years after which a view would be taken as to where the UIDAI would be located within Government.

first meeting of the EGoM

second meeting of the EGoM

third meeting of the EGoM

fourth meeting of the EGoM

e) Constitution of the UIDAI with a core team of 10 personnel at the central level and directed the Planning Commission to separately place a detailed proposal with the complete structure, rest of staff and organizational structure of UIDAI before the Cabinet Secretary for his consideration prior to seeking approval under normal procedure throughtheDoE/CCEA.

f) Approval to the constitution of the State UID Authorities simultaneously with the CentralUIDAI with a core teamof3personnel.

g) December 2009was given as the target date for UID to be made available for usage by an initial set of authorized users.

h) Prior to seeking approval for the complete organizational structure and full component of staff through DoE and CCEA as per existing procedure, the Cabinet Secretary should convene a meeting to finalize the detailed organizational structure, Staff and other requirements.

1.1. Subsequently, on January 22nd, 2009 the Cabinet Secretary in pursuance of the decisions of the Empowered Group of Ministers considered the proposal

submitted by the Department of InformationTechnology regarding the governance structure and recommended that

a) The notification for constitution of the UIDAI should be issued immediately.

b) A High Level Advisory, Monitoring and Review Committee headed by Deputy Chairman, Planning Commission to be constituted to over see the work of the authority.

c) A Member, Planning Commission or the Secretary, Planning Commission may be also assigned the task of looking after the work proposed of the Chief UID Commissioner.

d) CoreTeam to be put in place.

In pursuance of the Empowered group of Ministers' fourth meeting datedNovember4th, 2008, the was constituted and notified by the Planning. Commission on January 28th, 2009 as an attached office under the aegis of Planning Commission with an initial core teamof115officials.Therole and responsibilities of the UIDAI was laiddown in this notification. The UIDAI was given the responsibility to lay down plan and policies to implement UID scheme, and shall own and operate the UID database and be responsible for its updation and maintenance on an ongoing basis.

Subsequently on July 2nd,2009ShriNandan Nilekaniwas appointed as the Chairman of the UIDAI. Shri Nilekaniassumedchargeon23rdJuly,2009andsince then theUIDAI has started functioning. The Prime Minister's Council on UID Authority was constituted on 30th July, 2009 and its first meeting had taken place on 12th August, 2009. The Council endorsed the broad approach Submitted by the UIDAI.

Subsequently, the Government constituted a

Unique Identification Authority of India

Cabinet Committee on Unique Identification

Authority of India vide its order no 1/11/6/2009 dated 22nd October, 2009. The functions of this Committee, as per this notification are: All issues relating to the Unique identification Authority of India including its organisation, plans, policies, programmes, schemes, funding and methodology to be adopted for achieving the objectives of that Authority.

In 2007, the Planning Commission had recommended an approach to issuing unique identification numbers, where the enrolment into a Unique Identification (UID) database could be speeded up by using existing resident records in the databases of the Election Commission, PAN etc. This approach would speed up enrolment for those residents present in one of the aforementioned databases. These data bases however, may contain inaccuracies.

The model envisioned by the Unique Identification Authority of India (UIDAI) takes into account the inputs of the Planning Commission, as well as learnings from the previous approaches to identity. The detailed approach and the model of implementation is explained in subsequent chapters.

1.2 TheUIDAIapproach

The UIDAI implementation model

The model that the UIDAI envisions will have the reach and flexibility to enrol residents across the country. The UIDAI, as a statutory body, will be responsible for creating, administering and enforcing policy. The UIDAI will prescribe guidelines on the biometric technology, the various processes around enrolment, and verification procedures to be followed to enroll into theUID system.The UIDAI will also design and create the institutional microstructure to effectively implement the policy. This will include a Central ID Data.Repository (CIDR), which will manage the central system, and a network of Registrars who will establish resident touch points through Enrolling Agencies.

- The CIDR will be the central data repository, and will function as a Managed Service Provider. It will implement the core services around the UID – it will store resident records, issue unique identification numbers, and verify, authenticate and amend resident data.

  The CIDR will only hold the minimum information required to identify the resident and ensure no duplicates. This will include:

  TheUnique ID orUIDwill be a numeric that is unique across all 1.2 billion residents in India.

- The UID number will not contain intelligence. In older identity systems, it was customary to load the ID number with information related to the date of birth, as well as the location of the person.

  However this makes the number susceptible to fraud and theft, and migration of the resident quicklymakes location details out of date. The UID will be a random number.

  The UIDAI will also be collecting the following data fields and biometrics for issuing a UID:

  Name

  Date of birth

- Gender

  Father's/Husband's/ Guardian'sname and UID(optional for adult residents)

  Mother's/ Wife's/ Guardian'sname and UID(optional for adult residents)

  Introducer'sname and UID(in case of lack of documents)

  Address

  All ten finger prints, photograph and both iris scans

  2.1 TheCentral IdentitiesDataRepository (CIDR)

  2.2 TheUniqueIdentityNumber

  2.3 TheUniquelDagencies

The UIDAI will partner with a variety of agencies and service providers to enrol residents for UID numbers and verify their identity.

The structure of these UID agencies will be as follows:

Registrars will be State governments or central government agencies such as the Oil Ministry and LIC. Registrars may also be private sector participants such as banks and insurance firms.

The UIDAI will enter into memorandum of understandings' (MoUs) with individual Registrars, and enable their on-boarding into the UID system. The Registrars will need to make changes to their processes to be UID-ready. The UIDAI will support them in this, and in linking to the CIDR, connecting to the UID system, and adding UID fields to their databases.

The Registrar will take on the responsibility of ensuring that clean and correct data flows into the CIDR. Their key role in the system will be in aggregating enrolments from sub-registrars and enrolling agencies and forwarding it to the CIDR. Each Registrar will adopt UIDAI standards in the technology used for biometrics, as well as in collecting and verifying resident information, and submitting to audits.

Registrars –

The UIDAI will also enter into agreements with some Registrars for using the CIDR solely for authentication purposes. The service providers who will adopt the UID system for identity authentication during service delivery will follow certain processes and standards, and may need tore-engineer their internal processes. These will be the departments/entities that report to a specific Registrar. For instance, the line departments of the state government such as the RDPR (Rural Development and Panchayati Raj) department would be sub-registrars to the state government Registrar. Enrolling agencies will directly interact with and enrol residents into theCIDR. For example, the hospital where a baby is born would be

the 'enrolling agency' for the baby's UID,and would report to the municipality sub-registrar.

The UIDAI along with the Registrars will also partner with civil society groups and community networks which will promote the UID number and provide information on enrolment for hard to reach and marginalised populations.

The UIDAI's approach relies on the uniformity of standards in certain vital areas of operation. The Demographic data fields and verification procedure in the UID system as well as the Biometric standards to be utilized need to be standardized across the country and across the various registrars in the UID system. This is a sine qua non for the operability of the system. Hence, the UIDAI established two Committees to look into the issue of standards.

The UIDAI had constituted a Committee headed by Mr.N. Vittal, formerCVCon 9th October2009 to go into the question as to what demographic details should be collected from the residents for assigning of unique IDs. The Committee was also to go into the question as to what should be the process of verification of the residents at the time of their enrolment into the UID system. The mandate of the Committee was crucial because it isnecessary to ensure that the integrity and correctness of the data is not compromised while ensuring that the process of verification is non harassingto individuals. The Committee was mandated to give its report within 90 days of its constitution. However, it submitted its report on 9th December 2009,well before the ninety days' period given to it .The Report of the Committee has been accepted by the Authority. The Committee recommended the following data fields : Name, Date of birth, Gender, Father's/ Husband's/ Guardian's name and UID (optional for adult residents), Mother's/ Wife's/ Guardian's name and UID (optional for adult residents), Introducer's name and UID (in case of lack of documents) and Address. It has also specified the

verification process which broadly falls into three categories (i) Document-based, (ii) Introducer-based (in case of lack of documents) and (iii) Community-based verifications, a process which will be followed during the creation of NPR. The Report of the Vittal Committee is available atwww.uidai.gov.in

Sub-Registrars –

Enrolling Agencies –

Outreach Groups –

CommitteeonDemographicDataStandardsandVerificationProcedures

2.4 Setting standardsondemographic dataandbiometrics

CommitteeonBiometric Standards

As biometric attributes of the residents are going to be used as the basic signature for deduplication and to ensure uniqueness, it is necessary to go into the question as to what should be the type and specifications of biometrics to be collected at the time of enrolment. Therefore, a Biometrics Standards Committee, under the Chairmanship of the Director General of NIC, Dr. BK Gairola was constituted by the Authority on 29th September, 2009. This Committee was also expected to give its report within 90 days of its constitution. The Report was submitted on 7th January, 2010. The UIDAI has examined their Report and has accepted the standards for various biometric attributes as recommended by the committee as also various other recommendations related to collection of biometrics and their quality. The UIDAI has also decided that the face, all ten finger prints and both iris scans should be collected at the time of capturing the demographic and biometric details of a resident. This will be able to ensure uniqueness of the IDs at a scale of 1.2 billion residents.Thereport of the biometric committee is also available atwww.uidai.gov.in The UIDAI was declared as an Apex body to set standards in the areas of biometric and demographic data standards by the Prime Minister's Council of UIDAI. Now that both these standards have been finalized by the

UIDAI, these standards/specifications, processes and systems will be used by all the registrars to for enrolment of the residents into the UID system.

Enrolment into the UID system

Acritical aspect of the UID enrolment process is that enrolment will not be through a mandate, but will be demand driven. The momentum for the UID will come from residents enrolling in order to access the benefits and services associated with it. The basic advantage of the UID that can drive this demand, which will be communicated while promoting enrolment, is that the UID will be one number, which can be used to prove identity for life. Once the resident gets the unique ID, it may be accepted as identity proof across service providers.

The enrolment process for the UID number will begin with a resident submitting his/her information to the enrolling agency with supporting documents. This information will be verified according to the prescribed verification procedure as per the DDSVP Committee Report. To make sure the poor are not excluded, the UIDAI has prescribed guidelines for applicants without documents.

Once the enroller verifies the resident's information, it will submit the application request – either singly or in batches – through the Registrar to the CIDR. The CIDR will then run a de-duplication check, comparing the resident's biometric and demographic information to the records in the database toensure that the resident is not already enrolled. Since de-duplication also compares biometric records, itwould catch individuals enrolling with a different set of demographic details. The fact that the UID system is both de-duplicated and universal will discourage residents fromgiving incorrect data at the time of enrolment.

3.1 Theenrolmentprocess

Issuing theUIDnumber

Once the UID number is assigned, the UIDAI will forward the resident a letter which contains his/her registered demographic and biometric details. This letter

may also have ateara way portion which has the UID number, name, photograph and a 2D barcode of the finger print minutiae digest. If there are any mistakes in the demographic details, the resident can contact the relevant Registrar/enrolling agency as per a prescribed procedure.

If the Registrar issues a card to the resident, the UIDAI will recommend that the card contain the UID number, name and photograph. They will be free to add any more information related to their services (such as Customer ID by bank). They will also be free to print/ store the biometric collected from the applicant on the

- issued card. If more registrars store such biometric information in a single card format, the cards will become interoperable for offline verification.

But theUIDAI will not insist on, audit or enforce this.

All data entry that the enrolling agencies takeuponbehalf of theRegistrars will be done inEnglish. It can then be converted into the local language using standard transliteration software, and verified for accuracy by the Registrar. The letter the UIDAI sends the resident will consequently contain all demographic details in English as well as the local language of the state in which the resident resides. In this regard, the UIDAI will follow the precedent set by the Election Commission of India.

- The approach of the UIDAI to enrolment will be a pro-rural/pro-poor one. The Registrars targeted for rural India – the NREGA, PDS, Social security pensions - will be government agencies with large rural networks and significant bases among the poor. As a result, the UIDAI expects initial enrolment to be fairly rapid in both large and small rural areas.

3.2Enrolmentstrategyin ruralandurbanIndia

The enrolment strategy for urban India will include organizations which dominate services for urban residents, such as LIC and Passports. The table below summarizes the Registrars who are

- UID Registrar
- Primary
- Access1
- Additional
- Acces2
- Potential
- Overlap
- Effective
- Enrolment
- Crore Residents
- LPG (Oil PSU)
- LIC (Life Insurance)
- PAN Cards
- Passports
- Urban Enrolment
- Lic (Life Insurance)
- NREGA
- BPL Ration Cards
- State BPL/APL
- Old Age Pensioners
- Women/Child Welfare
- Social Welfare
- RSBY
- Rural Enrolment
- Total Enrolment
- 8.4
- 13.5

4.0
6.0
3.5
10.0
7.0
15.0
1.5
1.0
1.0
0.5
3 16.8
13.5
-
-
3.5
20.0
21.0
45.0
1.0
2.0
2.0
1.0
4 20%
50%
75%
80%
90%

10%

60%

50%

70%

70%

70%

70%

20.2

13.5

1.0

1.2

35.9

0.7

27.0

11.2

30.0

0.8

0.9

0.9

0.5

72.0

107.9

In addition to these enrollers, the UIDAI will also partner with the Registrar General of India (RGI)

– who will prepare the National Population Register through the Census 2011 -- to reach asmany residents as possible and enrol them into the UID database. This

may require incorporating some additional procedures intotheRGI data collection mechanism, in order tomake it UID-ready.

While the UIDAI intends to target Registrars that have large networks among the poor and rural communities in India, it will also emphasize multiple approaches to reach specific, frequently marginalized groups.

3.3 Afocused effort toenrol thepoorandhardtoreachgroups

These are residents who are part of the Registrar's customer / subsidiary beneficiary database and can be mandated to

- provide their UID

The residents under additional access are family members who can be easily covered while enrolling the primary residents.

These can be all family members in the case ofLPG connections and the nominees in case of LIC Policies.

The total number of gas connections is 10.51 crores,and this estimates that there are20%ineligible connections

Assuming there are an average of threemembersin each family having a gas connection from an Oil PSU

UrbanPoor

- Children

The urban poor are among the most ignored and disadvantaged people in India.

The main challenges in enrolment here exist because this group consists mainly of migrant workers with temporary or seasonal jobs.The following may be ways togetthe men rolled into theUID system.

Many of India's urban poor work as drivers, maids, or as workers associated with a family or a business. One approach to reach them could be for the head of the

family or business to enable these members (who are co-residents/co-workers) to get enrolled into the UID with the same address proof the business or family uses. There can be a host of financial incentives offered toenrol such co-residents.

The urban poor often borrow from micro-finance institutions and other sources and these could serve as enrolment points for them. There are established chit funds that can also act as enrolment points for theUIDtoimprove coverage. There are several established non-profits working in urban slums in education, healthcare and social empowerment. They can be used to educate the poor on the benefits of the UID, for actual enrolment and to help endorse identity for people who lack documentation. India is a young country with over 400 million residents belowthe age of 18. While family-based government schemes will as Registrars, help enrol children, this population may need to be specifically targeted.

ICDS is one of the world's largest integrated early childhood programs, with over 40,000 centers nationwide. The program covers over 5 million expectant and nursing mothers and 25 million children under the age of six. These centers can be information or enrolment points for non-school going children.

It may be mandated that at the time of joining school (first standard) it is necessary for children to have a UID or to enrol for one. This way the child can be tracked for progressandtargeted for direct benefits. The SSA program could also help enrol children in the 6-14 age group into the UID, which would also enable better child trackingandImprovements in the mid-day meal schemes.

For children, the advantages from the UID would be significant. Child-related programs in India have relied on often inaccurate, aggregate data at school/cluster/block levels, making these programs ineffective. The concept of Universal Child Tracking – the ability to track every child and ensure their all round development – is gaining ground. An accurate database of children with UIDs would be immensely beneficial to programs within theWomen and Child welfare as

well as the Education departments, which track development in anganwadis and progress of children in government schools,andwork toeliminate child labor.

Co-resident enrolment:

Financial institutions:

NGOs and Non-profits:

ICDS:

School admission:

Apart fromenrollers that are family-based government services in both urban and rural India such as PDS,RSBYetc, there needs tobe a strategy tocoverwomenoutside this net:

Robust collectives of women exist within micro-finance institutions and self-help groups across the country. Thesewould be important enrolment points forwomen. Organizations like Mahila Samakhya in the 9 states of Karnataka, Kerala, Andhra Pradesh, Gujarat, Uttar Pradesh, Uttar Khand, Assam and Jharkhand. Theywork in several thousand villages to help womenandcan act as touch points for education or enrolment ofwomen.

This is the apex national level organization of India for protecting and promoting the interests ofwomen. They have a massive outreach programthat can reach out to disadvantaged women and get them to enrol. The UID can subsequently be used as a unique handle for a variety of services tobe rendered tothesewomen.

It is estimated that India has over 60 million differently-abled people, and identity for this population is a massive challenge. The Disability Act of 1995 mandates a certain percentage of employment for the differently-abled, but without the clear identification of such individuals, it is difficult to enforce the law. There is an obvious incentive for organizations like National Center for Promotion of Employment for Disabled People (NCPEDP) to promote the UID, and enable

residents with disability to register for a range of benefits. The NGOs and rights groups associated withNCPEDPwould also be goodmechanismstoreach out tothis section of thepopulation. India has a significant tribal population of approximately 90 million tribals, mostly concentrated along a few states. The Government has many programs for the 697 notified tribes, which can be used for enrolment and information dissemination. In addition, NGOs and governments in states with hightribal populations can beRegistrars for tribal groups. Theabove mentioned approaches aremerely indicative of the strategy that theUIDAI will follow to reach marginalized groups. In addition, theUIDAI will reach out to other marginalized groups such as homeless people, individuals in shelter homes, remandhomes, asylums, etc. Enrolment costs can be thought of in two ways. One will be the cost to the enrolling agencies/Registrars for carrying out the enrolment process. The other costs will be to the residents tocometo the enrolment stations. Poormay have to forego theirwages for a day and also spendsometravel costs to travel to the enrolment stations The enrolment strategy will explore the **Financial institutions:**

The National Commission forWomen:

Civil SocietyOutreachstrategy

Women

Differently-abled people

Tribals

3.4 Enrolmentcosts

possibility of various mechanisms for funding the enrolment costs. TheRegistrars have the option here of charging for the cards they issue residents to offset enrolment costs. The UIDAI may issue guidelines aroundsuch pricing.

The UIDAI will periodically carry out a process audit of the information that comes in from the Registrars, to ensure data quality and that agencies are following guidelines recommended by the UIDAI. The audit would be on a random sample

- of residents, carried out either directly by the Authority or throughappointed agencies.Theauditmight focus on: Verification against scanned documents – The data contained in the resident records will be verified against the scanned documents. Physical document verification – The physical documents that are held by the Registrar will be validated against the electronic copies. Periodic process audits– Periodic audits will be carried out to at the enrolment sites, of the processesandsoftware.

- The UID number is a lifetime number, but the biometric information contained in the central database will have to be regularly updated. Children may have to update their biometric information every five years,while adults update their information every ten years.

- From time to time, the demographic information that the CIDR holds on the resident may also become outdated. Fields that are susceptible to change could be the 'present address' field, aswell as the resident's name (after marriage). There might also be an error in the fields that occurred during enrolment intotheUID. If a service provider authenticating or enrolling a resident finds, through its KYR process that the information provided by the resident (address, name, etc.) does not match with the UID record, or that the biometrics need to be renewed, it can ask the resident to update their information in the UID database. The service providermaymake the update a condition for the resident to receive the service/benefit.

- Enrolling agencies and Registrars can serve as points where the resident can update their UID fields. The resident will have to submit their new information at these updation points with the required documentary evidence. This may also include a biometric authentication prior to processing the request.

3.5 Ensuring cleanenrolmentdata fromRegistrars

3.6 UpdatingUIDdetails

Updating information with theUIDAI

3.7 Reaching criticalmassinenrolments

The Authority expects to start issuing the first set of UIDs between August 2010 to February 2011, and enrolment for the UID number is expected to reach a critical mass of around 200 million residents in two to three years. Until this point, the UIDAI will have to focus on generating demand from both Registrars and residents. However, once the critical mass is achieved, it will generate a network effect that drives demand and accelerates adoption among service providers and residents. And as more service providers across the country require the UID to dispense their services and benefits, adoption will ramp up rapidly. In four years, the UIDAI estimates that it will issue600millionUIDnumbers.

3.8Trackingenrolmentsacross the country

The UIDAI will employ a GIS internet-based visual reporting systemto track enrolment trends and patterns across India, as the project is rolled out across variousRegistrarsandstates.

The GIS system will showall UID enrolments by state, aswell as by Registrar. The system will also be able todrilldownwithin statesandintodistricts.

A challenge for full enrolment is registering the approximately 60,000 babies that are born in the country every day. Over the next several years, the UIDAI expects to enrol close to the entire Indian population. Once that goal is achieved, enrolment will reach a steady state,where only births (and deaths) aswell as immigrants need tobe recorded.

There are however, some challenges in registering new births. First, since their biometrics is not stable, they have to be re-scanned at a later age. Second, names are often not given in India at the timeof birth registration.

One way to ensure that the UID number is used by all government and private agencies is by inserting it into the birth certificate of the infant. Since the birth certificate is the original identity document, it is likely that this number will then persist as the key identifier through the individual's various life events, such as joining school, immunizations, voting etc. Since the name is a mandatory field in the UID database, it is essential that the child be given a name before applying for the UID number. This would ensure that the UID can also be allotted at birth. In the case of urban births, the municipality will be the enrolling authority and the UID Registrar can be the 'Registrar of Births, Deaths and Marriage' at the state level.

In rural areas, births take place at district or block level hospitals, in health care centersandathomesin the village.Thevillage accountant is theRegistrar of rural births, and he/she also issues the birth certificate and updates the information throughan enrolling agency.

3.9 Reachingasustainable, steady-stateinenrolment

TheUIDin the birth certificate

Biometricsandinfants

Recording deaths in theUIDsystem

The recording of unique individual biometrics in the UID database is a challenging one for infant records.Thesolution tothis is torecordtheUIDandbiometric of the parents in the child's record. The child's biometrics need to be taken at around 5 years of age, and updated in the UID system every 5 years until the age of 18. This will be enforced by an expiry date attached to the UID number, which will become invalid after that date. Until the time the biometric of the child stabilizes, any one of the parents/guardian will need to provide their biometric information for authentication.

It is also necessary to record deaths in the country, and the birth and death registration act provides for such registration. The same institutions that record births can be in charge of updating deaths in the UID system. The UID system will not remove a record upon the person's death; it will simply mark it as 'deceased' and hence will render it inactive for the purposes of authentication.

Ensuring strongauthentication,andwhat itmeansfor theUIDAI

The real test of reliability for the UID system will be during identity authentication. Confirming 'youarewhoyousay youare' remains the primary, often elusive goal of all Identity systems. The UIDAI approach – which will be online authentication, with biometric check – creates a very strong authentication system, and gives the UIDAI significant ability to confirm an individual's identity. The UIDAI will support the Registrars in building the infrastructure and systems necessary to authenticate residents in different parts of the country. This will be especially critical for Registrarsworking in rural areas and among the poor.

The speed of UID adoption in India depends on whether the number can help in elliminatingpoverty and marginalization, and in enabling greater transparency and efficiency in service delivery. If it succeeds in these goals, the number will become indispensible for residents in accessing services.

While the UID can provide the strongest form of pre-verification and identity authentication in the country, it cannot ensure that targeted benefit programs reach intended beneficiaries. The propoor impact of the UID, consequently, will nc gain tractlon unless there is a mechanism to link the UIDprocess with actual service delivery.

A clear adoption process can overcome this gap by helping introduce the UID method of authentication at every point of service delivery. To ensure this, the UIDAI will not onlywork with Registrars who do enrolment, but also with non-enrolling, service delivery agencies. Such agencies involved in the delivery of

services and benefits will be encouraged to partner with the UIDAI for authentication. Once they authenticate a resident's identity against the UID database every time they carry out a service transaction, they will be able to deliver services far more effectively.

In order to accommodate this authentication, agencies may need to re-engineer their business processes to be UID-enabled. The most basic requirement for change will be in incorporating the UID method of authentication into their systems. Agencies will have to adhere to norms and procedures specified by the UIDAI for fingerprint capture and verification, and introduce a robust biometric authentication process at every point of sale. There is tremendous value to be gained from widespread adoption of the UID for authentication, especially for residents. While enrolment in the UID database will ensure that residents are not denied access to fundamental services and rights because they cannot present positive proof of identity, adoption in authentication could go one step further, and ensure that residents

4.1 EnablingUIDadoption for authentication

consistently receive these services. This can include a wide range of benefits such as education, health coverage, old-age pensions and subsidized food grains, thereby fulfilling the UIDAI's pro poor agenda.

The UIDAI is only in the identity domain. The responsibility of tracking beneficiaries and the governance of service delivery will continue to remain with the respective agencies – the job of tracking distribution of food grains among BPL families for example, will remain with the state PDS department. The adoption of the UID will only ensure that the uniqueness and singularity of each resident is established and authenticated, thereby promoting equitable access to social services.The adoption of the UID during authentication will also have a direct correlation with subsequent enrolment. Greater enrolment comes fromthe value a

resident derives fromthe UID,which in turn depends on the rate of adoption. There is a positive cycle here, created from the relationshipbetween adoption and enrolment – the greater the adoption, the faster the enrolment and vice versa: The twin approaches of enrolment and adoption will result in greater influence and traction

for the UID among residents in the country, and establish the UIDAI as the only genuine identity authenticator in India.

There are multiple forms of authentication that the UID authority can offer. Certain types ofauthentication would have low to medium assurance if there is the possibility that the card is forged. Here we summarize the main forms of authentication, depending on the situation and equipment available.

is supportedby theUIDsystem. This can include - Online demographic authentication where the authenticating agency compares the UID number and demographic information of the UID holder to the information stored in the UID database.Theassurance level here ismedium.

- Online biometric authentication where the biometrics of the UID holder, his UID and key demographic details are compared to the details in the CIDR. The assurance level in this case is high.

- Online demographic/biometric authentication with API where the Registrar's backend system makes a programmatic call to the authentication APIs exposed by the UID system to perform authentication. The assurance level here may be medium-high depending on whether the check useddemographic or biometric inputs. may be supported by the Registrar, and does not use the authenticating service providedby theUIDAI. Thismaycomeintwoforms:

- Photo match authentication where the photo on the card is compared with the cardholder.

This is themostbasic formof authentication.Theassurance level here is low.

- Online authentication
- Offline authentication

4.2 Typesof authentication

- Offline biometric authentication compares the scanned fingerprint of the cardholder to the biometric storedontheRegistrar-issued card.Theassurance level here ismedium.

4.3 AuthenticationandtheUIDAI revenuemodel

Basic identity confirmation

- Addressverification

The ability of the UIDAI to offer agencies across the country strong, reliable authentication is the key to its sustainability. The UIDAI will offer resident authentication services for a fee to governmentsandprivate sector firms.

The agencies which request a resident authentication service will have to be registered with the UIDAIandfollowstrict guidelines in using the service aswell as in managing resident information.

Basic identity confirmation from the UIDAI would be free. In this transaction, the authenticator will provide the UID number, name and one other parameter such as date of birth of the person, andthe central database will confirm the identity as a

- 'Yes' or 'No' response. This type of transaction will be carried out in largenumbersandwill need quick response times. Chargeable authentication services can be oftwotypes: For security purposes, government agencies aswell as private sector firms require address proof from Indian residents before providing them with benefits and services. However, agencies often complain of the difficulty of address verification "you try to verify an address in India, and you enter a labyrinth". The service provider usually verifies address through a physical visit, aswell as an enquiry to confirm the other information

provided. This process is expensive and costs betweenRs.100andRs.500per verification.

The address authentication service the UIDAI will offer these entities would consequently be a valuable one. In the proposed transaction with the UID Authority, the agency will submit the UID, name and address of the resident to the CIDR, which will confirm the address. As a result, the agency will not have todophysical address verification. Services such as issuing a credit card or granting a loan need the confirmation of the resident's identity. This process for the resident involves the submission of photographs and other documentation confirming their identity. In the proposed transaction with the UID Authority, the agency can send the scanned photograph or fingerprint (based on the security level required) together with otherdemographic details toconfirm the identity of the person.

The following revenue model for the UIDAI is an illustrative one. It has been designed while keeping in mind the value the agency requesting authentication would derive from the service. The table below summarizes the kind of transaction, potential user agencies and the proposed transaction fee. Government agencies could be provided these services from the UIDAI at a subsidized rate.

1 Basic ID Confirmation Free Airlines during passenger check-in

2 AddressVerification Rs.5 Banks for account opening

3 Biometrics Confirmation Rs.10 Credit cards issue process

The authentication service from the UIDAI can begin after the initial bulk on-boarding of Registrars. The revenue estimates for the UIDAI below are based on the current expenditure of various agencies on KYR processes, which would be replaced by the Authority's authentication services. It also takes into account expected growth in demand for mobile connections, bank accounts, etc.

Sl. TransactionType TransactionFee PotentialUserAgencies

Biometrics confirmation

Revenueprojections fromauthentication services

UIDRevenueProjection TransactionType

(SteadyStateEstimates) Address Biometrics

NewMobile Connections 19.59 -

PANCards - 1.20

Gas ConnectionsbyPSU - 1.50

Passports 0.06 -

LICNewPolicies - 10.16

Credit Cards 0.70 -

BankAccounts 11.55 -

Airline Check-in --

ProjectedTotalTransactions 31.91 12.86

ProposedTransactionRate 5 10

TransactionRevenue 159.55 128.60

Estimated total annual revenue

at steady state (Rs. Crores) 288.15

- LegalFramework

The Constitution of India, through the Directive Principles of State Policy mandates that the state shall strive to minimize inequalities of income and endeavor to eliminate inequalities in status amongst individuals. The objective of the UIDAI is to solve the key problem of identity that individuals face and enable better and efficient delivery of services to the poor and marginalized so as to eliminate inequalities of income and status. It is therefore, imperative to have a proper legal structure in place to ensure the smooth functioning of the UIDAI. This section provides an overview of the legalandpolicy framework.

- The Unique Identification Authority of India (UIDAI) will be set up as a statutory body by an Act of Parliament.TheUIDAI will be authorized:.

o To collect the following identity information from any person voluntarily seeking a unique identity number:

Name

Date of Birth

Gender

Father'snameandUIDnumber

Mother'snameandUIDnumber

Address

All ten finger prints, photographhandboth iris scans

The lawwill contain a prescription against collecting any other information than the information permitted, with specific prohibitions against collection of information regarding religion, race, ethnicity, caste and other similar matters, and for the facilitation of analysis of the data for anyone or toengage in profiling or any similar activity.

o Toissue a unique identitynumbertothe personwhohas provided the necessary information andfulfilled the requirements as laiddownin rules prescribedby theUIDAI.

Art.38 (1) The State shall strive to promote thewelfare of the people by securing and protecting as effectively as it may a social order inwhich justice, social, economicandpolitical, shall informall the institutions of the national life.

(2) The State shall, in particular, strive to minimise the inequalities in income, and endeavour to eliminate

- inequalities in status, facilities and opportunities, not only amongst individuals but also amongst groups of people residing in different areas or engaged in different vocations.

o To verify the identity of any person at the time of the provision of information, the issuance of a unique identity number or at any other time per the UIDAI database or other possible means, as laiddownin rules prescribedby theUIDAI.

o To permit the UIDAI to set up or facilitate the infrastructure by which third parties can authenticate the identity of persons who have provided information to the UIDAI and the circumstances and conditions they can seek such verification. The information on the database will be used only toauthenticate identity.

o To establish or appoint a Central ID Data Repository (CIDR) for the purposes of collecting, managingandsecuring the databaseandtooutsource any such functions.

o To permit the appointment of Registrars in accordance with criteria laid down by the UIDAI to enrol people that seek unique identity numbers directly or indirectly through enrolling

agencies.

o To allow for the appointment of other service providers in accordance with criteria laid down by the UIDAI, as the UIDAI may deem fit to further its objectives and to ensure efficiency.

o To call for information and records, conduct inspections, inquiries and audit of the CIDR,Registrars, enrolling agenciesandservice providers..

o To enter into all necessary contracts and arrangements in order to fulfill the objectives of the UIDAI.

o Tosetupmechanismsfor grievance redressal for the public

o To setupa monitoring framework to improve implementation, create safeguards as required andstudy the impact of theUID

- o To hire the necessary technical and professional personnel necessary for executing the mandate andfulfill the objectives of theUIDAI.

Thelawwill also contain

- o Penal provisions against persons employed by, or associated directly or indirectly with, the CIDR, Registrars, enrolling agencies and other service providers for failing to comply with the directions issued under theAct
- o Penal provisions against persons employed by, or associated directly or indirectly with the UIDAI, CIDR, Registrars, enrolling agencies and other service providers for breach of certain key sections of the legislation – including the specific prohibitionsonprofiling, the disclosure of informationandmaintenance of confidentiality etc.
- o Penal provision for persons who intentionally or fraudulently provide wrong information, attempt to obtain a second unique identity number, steal the identity of any living or dead person, etc. In this context, there will be no liability on the part of the UIDAI or persons employed by, or associated directly or indirectly with the UIDAI, CIDR, Registrars, enrolling agencies and other service providers for providing a unique identitynumberto a personwho intentionally or fraudulently obtains suchnumber.

- The information that the UIDAI is seeking is already available with several agencies (public and private) in the country, the additional information being sought by the UIDAI are the finger prints and iris scans. However, the UIDAI recognizes that the right of privacy must be protected, and that people are sensitive to the idea of giving out their personal information, particularly the idea of information being stored in a central database to be used for authentication. UIDAI will protect the right to privacy of the person seeking the unique identity number. The information on the database will be used only to authenticate identity.

- Necessary provisions would be in place to address the issues of privacyandconfidentiality.

The UID database will be susceptible to attacks and leaks at various levels. The UIDAI must have enough teeth to be able to address and deal with these issues effectively. It will be an offence under theUIDAIAct toengage in the following activities:

Unauthorized disclosure of information by anyone in the UIDAI, Registrar or the Enrolling

- agency

Disclosure of information violating the protocols set in placeby theUIDAI

Sharing any of the dataonthe database with anyone.

Engaging in or facilitating analysis of the data for anyone.

Engaging in or facilltating profiling of any nature for anyone or providing information for profiling of any nature for anyone.

All offences under the Information Technology Act shall be deemed to be offences under the UIDAI if directed against theUIDAI or its database.

!

Protecting privacyandconfidentiality

- OffencesundertheUIDAIAct

DataSecurityandFraud

Even as the UIDAI stores resident information and confirms identity to authenticating agencies, it will have toensure the securityandprivacy of such information. By linking an individual's personal, identifying information to a UID, the UIDAI will be creating a transaction identity for each resident that is both verified and reliable. This means that the resident's identity will possess value,andenable the transfer ofmoney andresources.

under their name. issuingnumber. Person applies toget a second Application returned, with reason provided. cardin another name. If person'snamewas fraudulent the first time, he has the option of applying tochange his demographic fields. if this fraudis attempted again, person isaddedtowatch list/ legal action. Person appears as himself, Application returned, with reason provided. andapplies for a second If attemptedmore than three times person UIDnumber. addedtowatch list. Person appears as another Thevictim can report identity theft totheUIDAI'sexistingperson, registering grievance office.TheUIDAI will undertake an the second person's information investigation,andtake appropriate action if theft under his fingerprint. is confirmed. Impersonation of a deceased If the applicant passes the verification process,

individual, with fake supporting then hemay be able totakeonthe stolen identity. documents. However, he will not be able tochange hisdemographic fieldsover his lifetimewithoutdueprocess. De-duplicationworks incorrectly Person can request check against face biometrics andreturns false positive for aswell as re-verificationbyRegistrar. anewUIDapplicant.

Someof the potential fraudscenarios are:

Scenario Response

Technology architectureof theUIDAI

The technical architecture of the UIDAI is at this point, based on high-level assumptions. The architecture has been structured to ensure clear data verification, authentication and deduplication, while ensuring a highlevel of privacyandinformation security. The Central ID DataRepository will be the central database of all residents, containing the minimal set of fields sufficient to confirm identity. The federated set of databases belonging to the Registrars may contain additional information about the resident, and can use the resident's UID as the key.

under their name. issuingnumber. Person applies toget a second Application returned, with reason provided. cardin another name. If person'snamewas fraudulent the first time, he has the option of applying tochange his demographic fields. If this fraudis attempted again, person isaddedtowatch list/ legal action. Person appears as himself, Application returned, with reason provided. andapplies for a second If attemptedmore than three times person UIDnumber. addedtowatch list. Person appears as another Thevictim can report identity theft totheUIDAI'sexistingperson, registering grievance office.TheUIDAI will undertake an the second person's information investigation,andtake appropriate action if theft under his fingerprint. is confirmed. Impersonation of a deceased If the applicant passes the verification process,

individual, with fake supporting then hemay be able totakeonthe stolen identity. documents. However, he will not be able tochange hisdemographic fieldsover his lifetimewithoutdueprocess. De-duplicationworks incorrectly Person can request oheck against face biometrics andreturns false positive for aswell as re-verificationbyRegistrar. anewUIDapplicant.

Someof the potential fraudscenarios are:

Scenario Response

- Technology architectureof theUIDAI

The technical architecture of the UIDAI is at this point, based on high-level assumptions. The architecture has been structured to ensure clear data verification, authentication and deduplication, while ensuring a highlevel of privacyandinformation security. The Central ID DataRepository will be the central database of all residents, containing the minimal set of fields sufficient to confirm identity. The federated set of databases belonging to the Registrars may contain additional information about the resident, and can use the resident's.UID as the key.

7 Systemarchitecture

Thekey technologycomponents of theUIDsystemare:

which provides the enrolment and the authentication service. These services will be available over the network for the various Registrars and their authenticating agencies to use. The backend servers need to be architected for the high

I The UID Server,

demands of the 1:N biometric de-duplication as well as the large peak loads from authentication requests. is central to the UID system for enrolling as well as authenticating residents. It is likely that a multi-modal biometric solution will be used to achieve a high level of assurance. The 1:N de-duplication envisioned will be by far the most computing-intensive operation of the UID system. Innovative techniques of hashing, indexing, distributed processing, and in-memory databases using multiple-biometricmodesneed tobeemployed toget acceptable performance. application will capture and validate demographic and biometric data. This client needs to work in an offline mode in the village setting when there is no internet connectivity, and upload batch files to the server for processing. Alternatively the batch files can be physically transported to the CIDR for uploading The client application will be deployedona standardenrolmentworkstation.

is a critical aspect of the system, since all UID enrolment and authentication services will be available online. UID services could work over secure WAN networks, the vanilla internet or over mobile SMS channels. It could also potentially work over existing networks such as credit-cardPOS(point-of-service)devices. secures all the above components from logical/physical attack. Thisincludes .

o Server Security – firewall, intrusion preventionanddetection systems(IPS, IDS)

o Network, Client Security – Encryption, PKI etc

TheAdministration systemwill help administer theUIDAI's operations. This includes

o Account setup – creation/modification of Registrar, enrolling and authenticating agency accounts.

o Role based access control – Assign rightsoverUIDresources basedonrole.

o Audit trailing – track every access totheUIDsystem.

o Frauddetection – detect identity theftandcyber crimes using audit trails

o ReportingandAnalytics – Visual decision support tools – GIS, Charting etc.

- The Biometric sub-system
- The Enrolment client
- The Network
- The Security design

ProjectExecution

One of the unique challenges in executing the UID project is its scale. Due to the size of India's population, the UIDAI is undertaking what is perhaps the largest governance-related exercise in the world. We must ensure that all aspects of the project – enrolment, de-duplication, and authentication – function effectively even as thenumberof records approaches a billion. The UIDAI can expect its enrolment run-rate to have a peak load of one million enrolments per day in the very first year of operation. Every sub-systemand component of the UID systemwill need to scale quicklyandsignificantly. This will include: 1) The ability to onboard Registrars from different sectors and handle their constituencies of residents.

2) The legal framework of contracts needs to support the variety and spread of stakeholders as theirnumbersgrowexponentially across the country.

3) The biometric de-duplication algorithm needs to scale towards checking a fingerprint against everyone of 1.2 billion people toensure uniqueness.

4) The authenticating service, which may be used by tens of thousands of points across the country, needs toscale tohandlehundreds of thousands of transactions per second.

8.1 Addressing challenges of scale

Project Risk

1) Adoption risks:

2) Political risks:

3) Enrolment risks:

4) Risks of scale:

5) Technology risks:

6) Privacyandsecurity risks:

7) Sustainability risks:

The UID project does face certain risks in its implementation,which have to be addressed through its architectureandthe design of its incentives.Someof these risks include: There will have to be sufficient, early demand from residents for the UID number. Without critical mass among key demographic groups (the rural and the poor) the number will not be successful in the long term. To ensure this, the UIDAI will have to model de-duplication and authentication to be both effective and viable for participating agencies andservice providers.

The UID project will require support from state governments across India. The project will also require sufficient support from individual government departments, especially in linking public services to the UID, and from service providers joining as Registrars.

The project will have to be carefully designed to address risks of low enrolment – such as creating sufficient touch points in rural areas, enabling and motivating Registrars, ensuring that documentary requirements don't derail enrolment in disadvantaged communities – as well as managing difficulties in

address verification, name standards, lack of informationondate of birth,andhardtorecordfingerprints. The project will have to handle records that approach one billion in number. This creates significant risks in biometric de-duplication as well as in administration, storage,andcontinued expansion of infrastructure. Technology is a key part of the UID program, and this is the first time in theworld that storage, authentication and de-duplication of biometrics are being attemptedon this scale. The authority will have to address the risks carefully – by choosing the right technology in the architecture, biometrics, and data management tools; managing obsolescence and data quality; designing the transaction services model and innovating towards the best possible result.

The UIDAI will have to ensure that resident data is not shared or compromised.

The economic model for the UIDAI will have to be designed to be sustainable in the long-term, and ensure that the project can adhere to the standards mandatedby theAuthority.

UID-enabledmicro-paymentarchitecture

This section discusses one of the potential applications of the UID – the use of the number in driving financial inclusion, and in enabling a micropayments solution that the poor can use to access financial services.

While the demand for financial inclusion has gained urgency over the last few years, initiatives in India to expand financial infrastructure date back several decades, since the building of rural cooperative credit banks in the 1950s, and the spread of bank networks in the 1970s and 1980s.

These initiatives have paid off over the years — India's bank branches are well-networked, particularly across urban India.

But despite these efforts, access to finance has remained scarce in rural India, and for the poorest residents in the country. Today, the proportion of rural

residentswho lack access to bank accounts remains at 40%, and this rises to over three-fifths of the population in the east and north-east of India.

This exclusion is unfortunate. Economic opportunity is after all, intertwined with financial access. Such financial access is especially valuable for the poor — it offers a cushion to a group whose incomes are often volatile and small. It gives them opportunities to build savings, insure themselves against income shocks and make investments. Such savings and insurance protect the poor against potentially ruinous events—illness, loss of employment, droughts, and crop failures. However due to the lack of access to financial services, many of the Indian poor face difficulties in accumulating savings.

To mitigate the lack of financial access in India, the RBI has focused on improving the reach of financial services in new and innovative ways—through no-frills accounts, the liberalization of banking and ATM policies, and branchless banking with business correspondents2 (BC), which enables local intermediaries such as self-help groups, post offices and kirana stores to provide banking services. These efforts have also included the promotion of core-banking solutions in regional rural banks; and the incorporation of the National Payment Corporation of India (NPCI) as an apex switch, forpaymentsandsettlements.

In recent years, ATM and core banking, as well as greater mobile connectivity have also become two powerful engines of financial access. Mobile phones in particular present an enormous opportunity in spreading financial services across India. These technologies have reduced the need for banks to be physically close to their customers, and banks have been consequently able to experiment with providing services through online as well as mobile banking. These options, in addition to ATMs, have made banking accessible and affordable for many urban non-poor residents across the country.

With the poor however, banks face a fundamental challenge that limits the success of these technologies and recent banking innovations. The lack of clear identity documentation for the poor creates substantial difficulties in establishing their identity to banks. This has limited the extent towhichwe can leverage onlineandmobile banking toreach these communities.Besides challenges in access and identity, a third limitation has been the cost of providing banking services for the poor. The poor have unique preferenceswhen it comes to withdrawing money and making deposits—they prefer to do large numbers of small transactions, in 'micropayments' of say, Rs.10 rather than Rs.100. Banks discourage such payments, as transaction costs under this model would be too high to bear. The Unique Identification number (UID), which identifies individuals uniquely on the basis of their demographic information and biometrics, gives individuals the means to clearly establish their identity to public and private agencies across the country. It also creates an opportunity to address the existing limitations in financial inclusion. The UID, once it's linked to a bank account, can help poor residents easily establish their identity to banking institutions. As a result, the UID enables banking institutions to bring together the infrastructure thatnowexists in order tobuild an accessible, low-cost micropayments model.

Since the UID enables remote authentication of identity, it empowers the poor in making electronic transactions in small, micro-amounts, remotely and at low-cost, through BC networks connected by mobile phones. The model would thus be accessible and affordable across the country. Such a UID-enabled micropayments approach can bring about universal financial access for the poor — they would be able to access their accounts on the move, wherever they are, through any mobile phone, from any BC or bank. The UID-enabled bank account can thus be a global address for residents, similar toan email id or a mobilephonenumber. Over the last few years, we have seen critical reforms

implemented towards creating a payments solution for the poor. The UID number helps integrate these reforms and leverage the technology already in place into an effective micropayments solution. This can bring low-cost access to financial services toeveryone, a short distance fromtheir homes.

Banks in India are required to follow customer identification procedures while opening new accounts, to reduce the risk of fraud and money laundering. The strong authentication that the UID offers, combined with its KYR standards, could remove the need for such individual KYC by banking institutions for basic, no-frills accounts. It will thus vastly reduce the documentation the poor are required to produce for a bank account, and significantly bringdownKYCcosts forbanks.

The UID's authentication processes will allow banking institutions to verify poor residents both in person and remotely. Rural residents will be able to transact electronically with each other as well as with individuals and firms outside the village, reducing their dependenceoncash.

UID KYR sufficient for KYC:

Electronic transactions:

10.1 Features of UID-enabledmicropayments

Ubiquitous BC network and BC choice:

A high-volume, low-cost revenue approach:

For residents:

For the government:

For banking institutions:

The UID's clear authentication and verification processes will allow banking institutions to network with village-based BCs such as self-help groups, post offices and kirana stores. Customers will be able to withdraw money and make deposits at the local BC. Multiple BCs at the local level will also give customers a choice of BCs. This would make customers, particularly in villages,

less vulnerable to local power structures, and lower the risk of being exploitedby BCs.

The UID will mitigate the high customer acquisition costs, high transaction costs and fixed IT costs that we now face in bringing bank accounts tothe poor. No-frills accounts that can be provided and accessed at lowcost through local Bcs, with electronic cash transfers, would encourage large numbers of small transactions across these accounts, and make these accounts an important source of revenue forbanks. The UID-enabled Bank Account (UEBA) will bring financial access andaffordability to millions of residentswho are presently excluded from formal financial systems. A UID-enabled bank account will also help residents make cheaper, faster electronic transactions and remittances in the form of micropayments. The solution will enable universal access to their account from any bank or BC, and through any mobile device, enabling residents to access payments on the move. Regular, affordable access to banking services would also give the poor a means of keeping their money safe — a convenience that has long been available to the middle classwouldnowbe accessible tothe ruralandurban poor. Large-scale financial inclusion can pave the way for electronic benefit transfers (EBTs) for residents. Central and state governments will be able to eliminate the identity-related fraud that exists within its public programs with such transfers going into UIDenabled bank accounts. The bulk of the informal cash economy across rural India, and remittances between urban and rural India will also become part of the formal banking system, with traceable and accountable money flows. This will ensure compliance with Anti-Money Laundering laws and Financial Action Task Force standards. The government will gain these benefits without having to overhaul governance systems — the micropayments approach won't require governments to change decision-making processes across the central, stateandlocal level. The use of the central payments switch to move cash

tronically at the last mile will dramatically cut down on cash handling and transaction costs for banking institutions. The cost of customer acquisition would also be significantly reduced, as a resident with aUIDwould requirenofurther identification toget a UID-enabledbank account. A low-cost micropayment approach will make the large volume of micropayments, remittances and government transfers to UID-enabled bank accounts important sources of revenue for banking institutions. Through the BC network, banks would be able to access customers through

10.2 Benefits

the large distribution channels in the country—including the mobile prepaid network, post officenetwork and FMCG retailers. In addition, BCswould see increased revenues from larger numbers of micro-transactions.

Over the last decade, we have seen a transformation in financial access for residents across the country—the reforms that encouraged the expansion of ATM, internet and mobile banking have madefinancial access affordableandaccessible for largenumbersof residents. The transformation however, has been most significant for India's urban, non-poor residents. These policies have not addressed the unique challenges the poor face in financial access, and they consequently, remain at the peripherywhenitcomestoeffective access tofinance. The UID-enabled micropayments solution is just one of themany developmental applications that the UID number can enable. It is also a critically important application, which can help address India's financial divide. Linking the UID number to a universal, accessible, and affordable micropaymentsmodelcan transformthe access the poor have tobanking services in the country.

UID-enabled micropayments can be a stepping stone to creating economic opportunities for residents across the country, regardless of where they live. The financial inclusion that it makes possible will be critical to improving access for the

poor to resources and skills. As we move towards an open access society, it is this soft infrastructure—connectivity, financial inclusion, and identity—that will ultimately, empower the individual in India.

10.3 Conclusion

Over the last decade, we have seen a transformation in financial access for residents across the country—the reforms that encouraged the expansion of ATM, internet and mobile banking have madefinancial access affordableandaccessible for largenumbersof residents. The transformation however, has been most significant for India's urban, non-poor residents. These policies have not addressed the unique challenges the poor face in financial access, and they consequently, remain at the peripherywhenitcomestoeffective access tofinance. The UID-enabled micropayments solution is just one of themany developmental applications that the UID number can enable. It is also a critically important application, which can help address India's financial divide. Linking the UID number to a universal, accessible, and affordable micropaymentsmodelcan transformthe access the poor have tobanking services in the country.

UID-enabled micropayments can be a stepping stone to creating economic opportunities for residents across the country, regardless of where they live. The financial inclusion that it makes possible will be critical to improving access for the poor to resources and skills. As we move towards an open access society, it is this soft infrastructure—connectivity, financial inclusion, and identity—that will ultimately,empower the individual in India.

ANNEXURE P-16

Data Protection and Security Guidelines for Registrars

1. Background

This document lays down the data protection and security guidelines to be followed by Registrars of the Unique Identification Authority of India (UIDAI). Since the Aadhaar enrolment process and the enrolment for the services of the Registrar is common, it is essential to define the parameters of responsibility of UIDAI and the Registrars.

There are two components to the enrolment process:

a) Enrolment for Aadhaar - for which the resident provides their name, date of birth, gender, address and other optional fields such as mobile number , e-mail etc along with biometrics, namely, Photograph, 10 Finger prints and Iris. UIDAI will be responsible for safe custody of the information collected for the purpose of Aadhaar generation once it reaches CIDR.

b) Enrolment for the Registrars services - In addition to the information being collected by UIDAI, the

Registrars may also be collecting a wide range of information together with biometrics and the Aadhaar number in order to deliver their services to the residents. This information could be viewed as personal information. Hence, ensuring the confidentiality and security of this data is of great importance.

2. **UIDAI responsibility for - data protection and security**

UIDAI is capturing biometrics and demographics information to issue Aadhaar numbers to the residents and to authenticate the identity of an Aadhaar number holder. It is the responsibility of UIDAI to ensure safety and security of the data collected for Aadhaar enrolment. The data captured (demographic and biometric) shall at the point of collection be encrypted and transported to the Central Identities Data Repository where the UIDAI will decrypt the data in a secure location and use it for the purpose of de-duplication and subsequently for authentication. UIDAI will have a security policy in place which will detail and define the security protocols and access protocols to ensure safety of the data. It is the responsibility of the UIDAI to ensure the safety, security

and confidentiality of the data from the point of receipt and in the CIDR and to protect the data from unauthorised access and misuse.

3. Registrars responsibility for-data protection and security

The Aadhaar enrolments will be done through the Registrars. The Registrars will also be collecting additional data from the resident in order to deliver their services to the resident. This relationship between the resident and the Registrar is independent of the UIDAI. As a consequence Registrars have a fiduciary responsibility and has to exercise a duty of care to secure and protect all the data (demographic and biometric) collected from the resident. UIDAI prescribes the following broad measures for data protection and security to be adopted by Registrars:

a) Care in collection:

- Registrars shall take all necessary precautions, in respect of information received or collected by it so as to ensure such information is properly and accurately recorded, collated and processed;

b) Process for access and updating:

- Registrars shall also establish and adopt procedures to disclose to a person, upon their request, their own information-subject to satisfactory identification (in order to ensure that information is not revealed to third parties)

c) Principles and procedures relating to data collection, use and processing

- Registrars must collect information from residents only for the purpose related to their functions.
- The individual from whom data is being collected should be informed of the purpose for which information is being collected and how the data will be used.
- Registrars should obtain appropriate and clear legal consent from the resident.
- Registrars must ensure that data collected and maintained by them is protected against any loss, or unauthorized access; or use, or modification or disclosure.

- Data provided by the resident to a Registrar should be used by the Registrar for the purpose envisaged. Resident must be made aware of any data sharing policies of the Registrar. While some form of sharing maybe part of the governance framework of governments - residents must be made aware of the same. Any other sharing beyond the governance framework must only be done with the explicit consent of the resident and for the explicit reason for which the consent is given.

d) Data security protocols

- Security protocols should be in place from the point of collection, transmission of data and to the final destination/ facility where the data will be stored.

- Data must be housed in a secure facility with appropriate access controls and audit trails.

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful collection and processing of data and against accidental loss or destruction of, or damage to data.

e) Data retention policy

- Registrars must define the time period for which data is being collected and will be retained by them. Data should not be retained for longer than the purpose for which it was meant to be used.
- Data must not be made available for the use of or be retained by third party service providers such as enrolling agencies or by any other unauthorised personnel.
- Registrars must develop their own guidelines for preservation and destruction of data and records according to their functional needs.

4. **Security framework for Biometric data**

While the above broad guidelines are applicable for all forms of data collected from the residents, special care needs to be taken to address the security of biometrk information. Biometrics is unique to an individual and therefore is sensitive information that needs to be protected with the highest standard of care to thwart any possibility of misuse.

The biometric data will be encrypted immediately upon capture during the enrolment process. The data packet will be encrypted with the Registrars key. The Registrar is responsible for the secure transmission of the data and for storing the data at a secure location protected from unauthorised access and misuse. The Registrar is liable to the resident and the public at large for safety, security and proper use of the Biometric data collected by it. The following guidelines are prescribed for the Registrars for security protocols relating to biometric information of the residents.

4.1 Guidelines

1. Registrars should inform residents what biometric data is being collected and how the data will be used.

2. Develop data use and retention policies - Registrars should not collect and retain more data than they need for their purpose (if they want to issue cards and store finger print they should retain that data only and not the rest). Information that is not required must not be retained by them.

3. Registrars should develop data security policies and build up systems to ensure safe keeping of biometric data, protect from malware, spyware and hacking of systems, including access protocols, etc. For this purpose:

- Registrars must have a physically secure location (data centre) where the biometric data can be housed, with strict security protocols and protection from unauthorised access. Physical, network and application security must be taken care of.
- Biometric Data should always be stored in encrypted form. Data should not lie unencrypted at rest.
- Biometric Data should not be decrypted except for the time when it is being used.
- Only data that is required should be retained and the rest should be destroyed.
- Key management systems with logging and audit trails should be created preferably using a Hardware Security Module (HSM).
- Independent audit of the security facilities, processes and policies should be done periodically

and reports should be published to assure the public of the safety standards being followed.

4. Biometric data should not be made available to or be retained by enrolling agencies, at user points or by any other unauthorised personnel.

5. **Key technical safeguards**

Overall objective

To ensure that all UIDAI Registrars meet a minimum level of security when they store, process and transmit resident data the UIDAI has prescribed following control objectives and recommendations to meet them :

Control Objectives	UIDAI Recommendations
Maintain an Information Security Policy	Maintain a policy that addresses information security
Maintain a Vulnerability Management Program	Use and regularly update anti-virus software on all systems commonly affected by malware
	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Restrict access to resident data by business need-to-know
	Assign a unique ID to each person with
	computer access
	Restrict physical access to resident data

Build and Maintain a Secure Network	Install and maintain a firewall configuration to protect resident data
	Do not use vendor-supplied defaults for system passwords and other security parameters
Regularly Monitor and Test Networks	Track and monitor all access the network resources and resident data
	Regularly test security systems and processes
Protect Resident Data	Protect stored resident data
	Encrypt transmission of resident data across open, public networks

Maintain an Information Security Policy

Registrars must create and maintain an information security policy, which addresses the security requirements arising out as a result of their functional/ business needs and objectives. The objectives of this security policy are to:

- Provide management direction and support for information security.
- Provide a baseline for information security. Partner will have the flexibility to modify components of the operational framework to take into account specific business objectives and security requirements.

- Ensure appropriate safeguards and procedures are adopted to protect information and associated information technology resources
- Ensure that persons handling information are aware of their accountability and responsibilities

This policy shall be implemented through a process approach, based on the PDCA (Plan, Do, Check, Act) as follows. Sample Policies and Procedures followed by other organizations are listed in the annexure .

- **Plan**

Establish a security policy, objectives, targets, processes and procedures relevant to managing risk, and information security to deliver results in accordance with the Partner's overall policies and objectives

- Do

Implement and operate the security policy, control processes and procedures.

- Check
Monitor, and review the Security policy, control processes and procedures

- Act

Take corrective and preventive actions based on audit and review to achieve continuous Improvements of the security plan.

Maintain a Vulnerability Management Program

Registrars must formulate risk assessment policies, and procedures. As a part of this, all assets must be listed, threats & vulnerabilities identified, and assessed, and mitigation plan implemented for all threats. As a result of this, all vulnerable and high risk components would be identified, and protected. Some specific recommendations that may come out of such an exercise include:

- Use and regularly update anti-virus software on all systems commonly affected by malware. This includes all anti-spyware, anti-virus, and other host protection systems.

- Develop and maintain secure systems and applications. This includes the adoption of a secure software development life cycle.

Implement Strong Access Control Measures

Registrars must identify all information assets, and how they are used in their system. This must be followed by the following actions:

- Restrict access to resident data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to resident data

Access control must include physical, host (computer), and network security.

Build and Maintain a Secure Network

It is essential that a secure network be established to protect the system from attack, and misuse. Some sample guidelines for securing this network include:

- Install and maintain a firewall configuration to protect resident data. A firewall is required to prevent external, potentially malicious intruders from accessing the network, and the resources within.

393

- Do not use vendor-supplied defaults for system passwords and other security parameters. A commonly ignored aspect of security is that various systems come with default security parameters including passwords. Having them set to default values would allow intruders to access the network, and steal data / inflict damage.

Regularly Monitor and Test Networks

Once a secure network is established, it must be regularly monitored, and steps must be taken to keep it up-to -date for all security issues. Some possible mechanisms to ensure this include:

- Track and monitor all access to network resources and resident data

- Regularly test security systems and processes

- Regular security audits, and penetration tests for all systems, networks, and processes will help to keep security up to date with current threats, and ensure that no complacency sets in.

Protect Resident Data

From the resident's perspective, the primary purpose of all security plans is to ensure that the resident's data is not stolen, vandalized, or compromised in any way. To accomplish this, in addition to all the previous steps, the Registrar must classify resident data based on value, and usage. Further, a cryptographic system must be put in place

- Encrypt resident data at rest: i.e. all resident data must be encrypted, while it is stored on external or internal secondary storage.
- Encrypt resident data in motion: i.e. all resident data must be encrypted while it is being transmitted across open public networks (or even closed networks).
- Protect unencrypted data: i.e. while the data is in the host memory, unencrypted, the host system must be protected from malicious activity, including viruses, spy ware, etc.

6. Compliance

Compliance can be summarized into 3 stages:

Collecting and storing: Secure collection and tamper-proof storage of all log data so that it is available for analysis.

Reporting: Being able to prove compliance on the spot if audited and present evidence that controls are in place for protecting data.

Monitoring and alerting: Have systems in place such as auto-alerting, to help administrators constantly monitor access and usage of data. Administrators are warned of problems immediately and can rapidly address them. These systems should also extend to the log data itself - there must be proof that log data is being collected and stored. Compliance can be accessed through the use of an annual onsite data security audits, and quarterly network scans.

Annexure: List of Sample Policies which the Registrars must have in place:

- Information Security & Management Policy
- Information Security Organization Structure Policy
- Risk Assessment Policy & Procedures
- Asset Classification Policy and Procedure

- Asset Classification and control standard
- Information labeling and handling procedure
- Acceptable Use Guideline
- Procedure for control of documents and records
- Human Resources Security Policy and Procedure
- Physical and Environmental Security Policy and Procedure
- Change Management Policy and Procedure
- Third Party Management Policy and Procedure
- Antivirus and Malicious Software Policy and Procedure
- Backup and Restore Policy and Procedure
- Network Security Policy and Procedure (Including internet, intranet, mobile computing, tele-working, firewall security)
- Media Handling Policy and Procedure
- Monitoring Policy and Procedure
- Access Control Policy and Procedure (including password security)
- Network Access Control Policy and Procedure
- Systems Development Maintenance Policy and Procedure
- Incident Management Policy and Procedure

397

- Business Continuity Management Policy and Procedure
- Cryptographic procedure document
- Minimum Baseline Security Standards

//TRUE COPY//

398

ANNEXURE P-17

Govt. of India, Planning Commission
Unique Identification Authority of India (UIDAI)
New Delhi-110 001
F.No.13012/12/Legal/2012-UIDAI

13 March 2014

To,
Dr. Rajinder Singh,
Director,
Central Forensic Science Laboratory,
Central Bureau of Investigation,
Block No.4, CGO Complex,
New Delhi- 11 0003

Subject: Compliance of order of Hon'ble High Court in Criminal Writ Petition No.10 of 2014 filed by UIDAI in RC-7(S)2013, Goa

Sir,

With reference to your letter No.CFSL-2013/A-1711/0941 dated 12 March 2014, I am directed to bring to your notice that the direction of the Hon'ble High Court contains that "the legal aspect of the Right to Information and Right to Privacy shall be considered by the Court subject to ultimate decision of the Supreme Court in the above petition and other petitions pending before it".

In view of the above, you may please inform us the methodology by which your expert proposes to ascertain the technical capability of the system.

Yours faithfully,
Sd/-
Ashish Kumar
Assistant Director General

Copy for information to :

Head of Zone, Central Bureau of Investigation : Mumbai Zone, Tanna House, 11-A, Nathalal Parekh Marg, Colaba, Mumbai-400039 with reference to their confidential Memorandum No. 462/ RC07(S)/2013-Goa/HoZ/ CBI/ Mum./14 dated 5 March 2014 addressed to CFSL as appended to the letter referred above.

Sd/-
Ashish Kumar
Assistant Director General

//True Copy//

400

ANNEXURE P-18

Govt. of India, Planning Commission
Unique Identification Authority of India (UIDAI)
New Delhi-110 001

F.No.13012/12/Legal/2012-UIDAI 13 March 2014

To,

Dr. Rajinder Singh,
Director,
Central Forensic Science Laboratory,
Central Bureau of Investigation,
Block No.4, CGO Complex,
New Delhi- 11 0003

Subject: Compliance of order of Hon'ble High Court in. Criminal Writ Petition No. 10 of 2014 filed by UIDAI in RC-7(S)2013, Goa

Sir,

With reference to your letter No.CFSL-2013/A-1711/0941 dated 12 March 2014, I am directed to bring to your notice that the direction of the Hon'ble High Court contains that "the legal aspect of the Right to Information and Right to Privacy shall be considered by the Court subject to ultimate decision of the Supreme Court in the above petition and other petitions pending before it".

In view of the above, you may please inform us the methodology by which your expert proposes to ascertain the technical capability of the system.

Yours faithfully,
Sd/-
Ashish Kumar
Assistant Director General
//TRUE COPY//

401

Ashok Pal Singh
Deputy Director General

Govt. of India, Planning Commission
Unique Identification Authority of India
(UIDAI) New Delhi-110 001

DO No.26010/06/2011-Tech Dated: 13th March, 2014

Dear Javed,

As discussed, the privacy concerns of the individuals who have voluntarily enrolled for Aadhaar, as also the technical architecture of the Central Identities Data Repository (CIDR) of UIDAI, preclude random biometric search. On the privacy issue, the matter as you are aware, is before the Supreme Court in a host of Public Interest Litigation matters. As such, the CIDR of UIDAI is not of use for the investigative work of the CBI.

Regards,

Yours sincerely,
Sd/-
(Ashok Pal Singh)

Shri S. Javed Ahmad
Joint Director (P)
Central Bureau of Investigation
C.G.O. Complex, Lodhi Road
New Delhi-110003.

//TRUE COPY//

402

ANNEXURE-P-19

DATA SHARING POLICY

UIDAI embarked on a multi-Registrar model for enrolling the residents with the intent to have the reach and ability to enrol the residents at a reasonable pace.

Registrars are entities who, in the normal course of their activities, deal with residents in the delivery of benefits and services to them. The Registrars carried out enrolments under the aadhaar project through Enrolment Agencies appointed by them. These Registrars already have data bases and collect data from their customers/beneficiaries for discharging the responsibilities cast up on them under various policies, statutes or rules. The Registrars partnered with the UIDAI to avail the opportunity of cleansing their data bases through fresh enrolments of residents in accordance with the UIDAI processes.

In some States where the non-State Registrars were active, State Registrars are facing problems in leveraging aadhaar for delivery of benefits (which is the basic intent of aadhaar project) since data of residents of the State enrolled by the non-State Registrars was not available to

the State Registrars. Many State Registrars have had reservations about the involvement of Non State Registrars in the enrolment exercise in absence of any clarity as to how they would be able to access the data of residents enrolled by Non State Registrars. The Enrolment Refresh Committee had also mentioned about the need of sharing of data with such Registrars.

In such a scenario, a policy on data sharing policy assumes an important dimension; wherein on one side, there are concerns regarding privacy, data protection, data security, etc, and on the other hand, there is demand from various State Registrars for the data to enable them leverage the UID for improving the services.

With the above in consideration, it has been decided that UIDAI would share the Resident data, subject to the following conditions:

1. UIDAI would share the data only in such cases where the resident has given the consent for sharing data.

2. The data will be UID generated processed data.

3. The data will be shared on receipt of a formal request from the State concerned. The request will explicitly include the purpose for which the data is required and specific data requirements.

4. States may request data pertaining to their own state only. The data shared will be based on state specified in the resident address.

5. The selective data in specific format, as defined by UIDAI, will be shared as per the validity of the request in a secured manner using appropriate offline and/or online mechanisms.

6. The data would be shared with State Registrars only for the purpose of improvement of delivery of welfare and public services, it also being the intent behind the aadhaar project and the purpose for which the consent has been given by the resident at the time of enrolment.

7. Demographic data may be shared with Financial Institutions (Banks, etc) for opening of Bank accounts and/or linking the accounts with aadhaar,

as consented by the resident at the time of enrolment or subsequently.

8. Data may also be shared as warranted under any Act/ Statute/ Regulation of Govt of India and/or any Cabinet Decision in this regard.

9. State Registrars may use the shared data with their various departments for the purpose of improving delivery of their welfare and public services but the Nodal Department shall be responsible for ensuring Security compliance.

10. The Registrar packet will not be generated, if Registrar does not ask for it.

11. UIDAI may also consider enabling electronic KYC mechanism where an authorized entity can send a request to UIDAI to share demographic data and photo for a specific resident, in the long run. This mechanism will require the said entity to send resident data sharing consent along with resident authentication factor (biometric/OTP). UIDAI will share data after successful resident authentication. UIDAI will define set of authorized entities who will

be allowed to avail this service, at the appropriate time.

12. Updates should be allowed to flow to agencies with whom UIDAI shared the data initially as per resident consent from time to time.

13. The necessary framework and Institutional safeguards as per the IT Act 2000 and all guidelines/rules/enactments of the Government of India for ensuring the data safety and security at all times would be put in place by concerned Registrar before sharing of any data. Registrar will sign a "Data protection and Understanding, of holding sensitive data" agreement with UIDAI. Among other things, the Agreement will include various required compliances for the following security guidelines and any other security guidelines as the UIDAI may deem fit:-

a. Strategic control of the data shall always remain with the Registrar who shall be responsible for the overall security and proper use of the data at all times.

407

b. Data shall be stored and transmitted in encrypted form.

c. Biometric data shall not be decrypted except for the time when it is being used. Under no circumstances, the biometric data of a resident shall be sent as part of any response to any verification request.

d. Registrar shall have a physically secure location to store /house the shared data, with strict security protocols and protection from unauthorised access. The facility should have appropriate access control and audit trails.

e. Physical, Network and Application level security for the software that uses this data shall be ensured.

f. State Registrar shall remove the biometric data if "resident" moves out of the state and informs the state.

g. The data should not be retained beyond the duration necessary to serve the purpose for which it was meant to be used.

h. Failure to comply with any of above obligation shall be deemed a serious breach by the Registrar concerned with whom data was shared by UIDAI and the said Registrar shall destroy the shared data within the time specified by UIDAI, without prejudice to any damages, which UIDAI may seek.

//TRUE COPY//

IN THE SUPREME COURT OF INDIA

CRIMINAL APPELLATE JURISDICTION

CRL.M.P.NO._____OF 2014

IN

SPECIAL LEAVE PETITION (CR.) NO. OF 2014

IN THE MATTER OF:

Unique Identification Authority of, . Petitioners

India &Anr.

V.

CBI - Goa & Anr. .. Respondents

APPLICATION FOR EXEMPTION FROM FILING THE CERTIFIED COPY OF ORDER DATED 26.02.2014 AND OTHER ANNEXURES IN PRESCRIBED FORMAT

To,

The Hon'ble Chief Justice India and his
Companion Justice of the Supreme Court of India
At New Delhi

The humble Petition of the above Named petitioner:

MOST RESPECTFULLY SHOWETH:

1. That the Petitioner No.1 has filed the accompanying special leave petition under article 136 of the Constitution of India against the

impugned order dated 26.02.2014 passed by the Hon'ble High Bombay at Goa in Criminal Writ Petition No.10 of 2014. All the facts of the case are set out in detail in the synopsis and list of dates and memo of special leave petition. Therefore same are not being repeated for the sake of brevity.

2. That the fact stated in the special leave petition may be read as part and parcel of the special leave petition and the same have not been repeated herein for the sake of brevity:

3. That the certified copy of the order dated 26.012014 is not available as the Petitioner had applied for the same and due to constraint of time and urgency in filing of, fair typed copies of the Annexures are not ready Therefore, as soon as the petitioner will receive the fair typed copies of the annexure, the Petitioners will file the same in the Hon'ble Court.

It is therefore, most humbly prayed that Hon'ble Court may kindly grant the exemption to the applicant from filing the certified copies of the annexure and fair typed copies of the annexure annexed with the accompanying Special Leave Petition.

PRAYER:

It is, therefore, most respectfully prayed that this Hon'ble Court may graciously be pleased to:

(i) Allow the present application in the interest of justice and exempt the petitioner for filing the certified copy of the order and other documents in the prescribed format.

(ii) Pass such and further order as this Hon'ble Court deems fit and proper in the circumstances of the case.

DRAWN BY

DRAWN ON

FILED ON

FILED BY

(D.S. MAHRA)
Advocate-on-Record for Petitioners